MTR070050

MITRE TECHNICAL REPORT

Addressing Industrial Control Systems in NIST Special Publication 800-53

March 2007

Marshall D. Abrams

Sponsor:	National Institute of Standards and Technology	**Contract No.:**	TIRNO-99-D-00005
Dept. No.:	G027	**Project No.:**	19058066-DA
Tracking no.	07-0466		

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

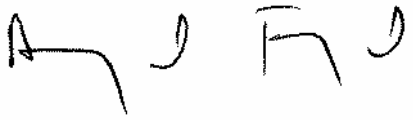
Approved for public release; distribution unlimited.

©2007 The MITRE Corporation. All Rights Reserved.

MITRE

Center for Enterprise Modernization
McLean, Virginia

MITRE Department
and Project Approval:



Amgad Fayad, G27 Department Head

Executive Summary

The Federal Information Security Management Act of 2002 (FISMA) directed federal agencies to promulgate federal standards for: (i) the security categorization of federal information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; and (ii) minimum security requirements for information and information systems in each such category. Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, mandates that agencies specify minimum security requirements for federal information and information systems. This standard specifies minimum security requirements for federal information and information systems in 17 security-related areas. Federal agencies must meet the minimum security requirements by using the security controls in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, as amended. Revision 1 to SP 800-53 was published in December 2006.

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability): LOW, MODERATE, and HIGH. The application of these definitions takes place within the context of each organization and the overall national interest. SP 800-53 defines sets of *baseline* controls as the minimum security controls recommended for an information system based on the system's security categorization in accordance with FIPS 199.

The overall objective of this report is to analyze how well SP 800-53 addresses cyber security in Industrial Control Systems (ICS), with particular focus on electric energy systems that are part of the nation's critical infrastructure. At the time this research was conducted, the only available comparable documents that addressed the cyber security of ICSs were the North American Electric Reliability Council's (NERC) series of cyber security standards, (Critical Infrastructure Protection [CIP]-002 through CIP-009)[1]. This report therefore focuses on comparing the NERC CIPs with SP 800-53. Specifically, this report:

- Develops a mapping between the security countermeasures in NIST SP 800-53 and the requirements in the NERC cyber security standards CIP-002 through CIP-009.
- Identifies areas of commonality and difference between SP 800-53 and the NERC cyber security standards.
- Determines the impact on an organization of conforming to both SP 800-53 and the NERC cyber security standards.
- Develops recommendations for NIST.

[1] http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection

Findings

- Most requirements in the NERC CIPs correspond to countermeasures in SP 800-53.
- "Measures" in the NERC CIPs correspond to "assessments," which are primarily addressed in SP 800-53A *Guide for Assessing the Security Controls in Federal Information Systems.*
- Compliance in the NERC CIP correspond to SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems.
- The Information Technology (IT) systems addressed by the NERC CIP paradigm are a subset of those addressed by the FISMA family of standards and guidelines.
- The requirements in the NERC CIPs are a subset of the Moderate Baseline set of controls in SP 800-53:
  - This subset is inadequate for protecting critical national infrastructure.
  - The Moderate Baseline is inadequate for all electric energy systems when the impact of regional and national power outages is considered.
- The objectives used for determining the importance of the IT systems addressed are narrower in the NERC CIP paradigm than the same types of objectives are in the FISMA family of standards and guidelines.
  - The FISMA family of standards and guidelines is concerned with the potential impact on an organization should certain events occur that jeopardize the information and information systems needed by the organization to:
    - Accomplish its assigned mission
    - Protect its assets
    - Fulfill its legal responsibilities
    - Maintain its day-to-day functions
    - Protect individuals
    - Control potential national-level impacts.
  - The NERC CIP are concerned with the reliability and operability of the Bulk Electric System, excluding:
    - Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission.
    - Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

- The Energy Policy Act of 2005 led to changes in the status and relationship of NERC and the Federal Energy Regulatory Commission (FERC):
  - The United States will no longer rely on voluntary compliance with electric industry reliability standards.
  - FERC is responsible for developing mandatory enforceable electric reliability standards.
  - NERC became FERC's Electric Reliability Organization (ERO)
  - FERC staff is reviewing all applicable voluntary standards previously developed by NERC.
  - FERC staff produced a preliminary assessment[2] of the NERC CIP that has been released for public review and comment.

Recommendations

- Organizations should create and maintain information security policies that are:
  - Germane to their mission and objectives
  - Flexible
  - Enforceable
  - Supporting of conformance reporting and remediation.
- Because the scope of the NERC CIPs is a subset of the FISMA scope, federal agencies should adhere to the FISMA scope.
- NIST and FERC should work together to develop an interpretation of SP 800-53 that is applicable to both public and private entities in the electric power sector.

[2] Federal Energy Regulatory Commission, *Staff Preliminary Assessment of the North American Electric Reliability Corporation's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection*, RM06-22-000, December 11, 2006. Available at http://www.ferc.gov/industries/electric/indus-act/reliability/12-11-06-cip.pdf

Table of Contents

1 Introduction 1-1

1.1 Purpose and Objectives 1-1

1.2 Background 1-2

1.2.1 SP 800-53 Overview 1-2

1.2.2 Industrial Control Systems Addressed in SP 800-53 1-3

1.2.3 Correspondence of NERC CIPs to NIST Standards and Guidelines 1-5

1.2.4 Industrial Control Systems and Critical Infrastructure 1-6

1.2.5 Background of NERC Critical Infrastructure Protection Standards 1-6

1.3 Document Organization 1-7

1.4 Relevant Professional Organizations 1-7

2 Findings and Recommendations 2-1

2.1 Cyber Security in the Industrial Process Control Community 2-1

2.1.1 Relationship among NERC CIP and NIST Publications 2-1

2.1.2 Comparing Documents from Different Organization Frameworks 2-18

2.1.3 Context of NIST Standards and Guidelines Addressing Cyber Security 2-18

2.1.4 When Multiple Paradigms Apply 2-20

2.1.5 Recommendation 2-21

2.2 Information Security Policy 2-22

2.2.1 Finding 2-22

2.2.2 Recommendation 2-22

2.3 Identifying Critical Information Technology 2-22

2.3.1 FISMA Paradigm 2-22

2.3.2 NERC CIP Paradigm 2-23

2.3.3 Comparison 2-23

2.3.4 Recommendations 2-24

Appendix A Relevant Federal Government Documents A-1

A.1 Federal Laws and Regulations A-1

A.2 Executive Orders A-1
A.3 Office of Management and Budget A-2
A.4 Department of Homeland Security (DHS) A-2
A.5 Department of Commerce (DOC) A-2
A.6 Government Accountability Office (GAO) A-7
A.7 Federal CIO Council A-7
A.8 Other Sources A-7
Appendix B Relationship between the NERC CIPs and SP 800-53 B-1
B.1 Challenges in Comparing Documents B-1
B.2 Requirements and Controls B-2
B.3 Scope B-2
B.4 Tables of Content B-4
B.5 Mapping NERC CIPs to Other NIST Publications B-12
B.6 Information Security Policies B-13
B.7 Criticality and System Definition B-14
B.8 Mapping Codes B-15
B.9 Row and Column Counts B-15
Appendix C Detailed Requirements Comparison between the NERC CIPs and SP 800-53 C-1
C.1 Documentation Requirements C-1
C.2 Assurance Requirements C-1
C.3 Detailed Requirements Comparison C-2
C.4 Operational Records and Corporate Governance Requirements C-42
C.5 Redundant Requirements C-43
Appendix D Glossary and Acronyms D-1
D.1 Glossary D-1
D.2 Acronyms D-7

List of Tables

Table 2-1. Where Security Concerns are Addressed 2-1
Table B-1. CIP Cyber Security Standards Requirements B-4
Table B-2. SP 800-53 Controls B-6
Table B-3. Mapping Codes B-15
Table B 4. NERC Cyber Security Standards Requirements B-17
Table C 1. Corresponding Requirements C-3
Table C 2. NERC CIP Operational Records and Corporate Governance Requirements C-42
Table C 3. Redundant NERC CIP Requirements C-43

1 Introduction

1.1 Purpose and Objectives

MITRE produced this report as part of independent advisory and technical support to the National Institute of Standards and Technology (NIST) Computer Security Division, which is developing standards and guidelines to support the Federal Information Security Management Act of 2002 (FISMA), Public Law 107-347 Section III, December 2002.

The overall objective of this report is to analyze how well SP 800-53 addresses cyber security in Industrial Control Systems (ICS), with particular focus on electric energy systems that are part of the nation's critical infrastructure. At the time this research was conducted, the only available comparable documents that addressed ICS cyber security were the North American Electric Reliability Council (NERC) series of critical infrastructure protection (CIP) cyber security standards (CIP-002 through CIP-009)[3]. This report therefore focuses on comparing the NERC CIPs with SP 800-53. Specifically, this report:

- Develops a mapping between the security countermeasures in NIST SP 800-53 and the requirements in the NERC cyber security standards
- Identifies areas of commonality and difference between SP 800-53 and the NERC cyber security standards
- Determines the impact on an organization of conforming to both SP 800-53 and the NERC cyber security standards
- Develops recommendations for NIST concerning steps to take to support the protection of critical infrastructure by converging standards

NIST Special Publication (SP) 800-53 Revision-1[4], *Recommended Security Controls for Federal Information Systems*, was published in December 2006. Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, delegates specifications of cyber security controls, or countermeasures, to SP 800-53. These specifications are binding on non-national security information and information systems that belong to, or are operated for, federal government agencies. The results are expected to influence a much wider circle, including regulatory agencies, some national security systems, and the private sector.

---

[3] http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection

[4] Hereafter in this report it is referred to as SP 800-53.

1.2 Background

This section provides an overview of SP 800-53, the context of NIST standards and guidelines addressing cyber security, and the NERC CIPs.

1.2.1 SP 800-53 Overview

SP 800-53 provides a comprehensive catalog of security controls for information and information systems. Security controls are the management, operational, and technical safeguards or countermeasures used to protect the confidentiality, integrity, and availability of a system and its information. NIST has established an annual review and update cycle for SP 800-53 to ensure that the countermeasures listed in the catalog represent the current state of the practice in safeguards and countermeasures for information systems.

The challenge for organizations is to select the appropriate set of security countermeasures to meet the specific, and sometimes unique, security requirements of that organization, thereby demonstrating the organization's commitment to security and due diligence. SP 800-53 provides sets of baseline controls to assist organizations in making the appropriate selection of countermeasures. Three sets of baselines–low, moderate, and high, based on security categories derived from FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*–are provided as starting points for organizations in determining the appropriate safeguards and countermeasures. Because the baselines are intended to be broadly applicable starting points, modifications to a selected baseline may be necessary in order to achieve adequate risk mitigation. Such modifications are tied to the risk assessment that extends and refines the FIPS 199 determination and documented in the security plan for the individual information system.

All NIST publications are issued in a dynamic context of laws and regulations. Appendix A of this document lists many of the federal regulations and guidance documents that help define the cyber security environment for federal agencies. The following two definitions are important in understanding SP 800-53:

- Information System– A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- Information Resources– Information and related resources, such as personnel, equipment, funds, and Information Technology (IT).

1.2.2 Industrial Control Systems Addressed in SP 800-53

Revision 1 of SP 800-53 introduced a new Appendix I that provides interim guidance on the application of the security controls to ICSs:

> Industrial control systems[5] are information systems that differ significantly from traditional administrative, mission support, and scientific data processing information systems. Industrial control systems have many unique characteristics—including a need for real-time response and extremely high availability, predictability, and reliability. These types of specialized systems are pervasive throughout the critical infrastructure, often being required to meet several and often conflicting safety, operational, performance, reliability, and security requirements such as: (i) minimizing risk to the health and safety of human beings; (ii) preventing serious damage to the environment; (iii) preventing serious production stoppages or slowdowns that result in negative impact to the nation's economy and ability to carry out critical functions; (iv) protecting the critical infrastructure from cyber attacks and common human error; and (v) safeguarding against the compromise of proprietary information.[6]
>
> Until recently, industrial control systems had little resemblance to traditional information systems in that they were isolated systems running proprietary software and control protocols. However, as these systems have been increasingly integrated more closely into mainstream organizational information and management systems to promote data sharing, connectivity, efficiency, and remote access capabilities, they have started to resemble the more traditional information systems. In many cases, industrial control systems are using the same commercially available hardware and software components as are used in the organization's traditional information systems. While the change in industrial control system architecture supports new information system capabilities, it also provides significantly less isolation for these systems from the outside world and introduces many of the same vulnerabilities that exist

---

[5] An industrial control system is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems that use programmable logic controllers (PLC)to control localized processes. Industrial control systems are typically found in the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries, as well as in air and rail transportation control systems.

[6] See Executive Order 13231 on Critical Infrastructure Protection, October 16, 2001.

in current networked information systems. The result is a greater need to secure industrial control systems.

FIPS 200, in combination with NIST Special Publication 800-53, requires that federal agencies implement minimum security controls for their organizational information systems based on the FIPS 199 security categorization of those systems. This includes implementing the minimum baselines described in Special Publication 800-53 in industrial control systems that are operated by or on behalf of federal agencies. This appendix discusses the problems that agencies may encounter in applying the security controls in Special Publication 800-53 to industrial control systems and provides some observations and recommendations on how to meet the intent of the requirements until NIST develops additional guidance specific to those types of systems. The specific guidance for industrial control systems may include modifications of the current security controls and control enhancements and/or interpretations of selected security controls for the specialized environments in which the controls are applied.

Because today's ICSs are a combination of legacy systems (which often have a planned life span of between 20 and 30 years), hybrids of legacy systems augmented with today's commercially available hardware and software, and are interconnected to other organizational information systems, it is often difficult or impossible to apply some of the security controls contained in SP 800-53. Recognizing this problem, NIST has initiated a high-priority project, in cooperation with the public and private sector ICS community, to develop specific guidance on the application of the security controls in SP 800-53 to ICSs. Because that ICS project is still ongoing, the resulting guidance could not be included in the current release of SP 800-53. However, based on the results of the project to date, NIST makes the following observations and recommendations for organizations that own and operate ICSs:

- Section 3.3 of SP 800-53, Tailoring the Initial Baseline, allows the organization to modify or adjust the recommended security control baselines when certain conditions exist that require that flexibility. Based on the discussion above, NIST recommends that ICS owners take advantage of the ability to tailor the initial baselines when it is not possible or feasible to implement specific security controls contained in the SP 800-53 baselines. However, all tailoring activity should, as its primary goal, focus on meeting the intent of the original security controls whenever possible or feasible. Additionally, the organization must address the residual risks present after the tailoring is completed.

- In some cases, it may be infeasible, impractical, or unsafe to implement a specific security control within an ICS. For example, AC-11, *Session Lock*, is required for all moderate-impact and high-impact information systems. For ICSs with requirements for real-time response and extremely high availability, predictability, and reliability, session lock may not make sense (e.g., locking an operator's session in an electric power

distribution system or an air traffic control system). However, the purpose of the session lock control is to prevent unauthorized access to an information system when the user or operator leaves the terminal or workstation unattended for a period of time. In this case, in order to meet the intent of the session lock security control, an organization could utilize the compensating control concept described in Section 3.3 of SP 800-53. With appropriate rationale as described in the compensating control section of SP 800-53, an organization can choose to compensate for not using session locks by incorporating other safeguards and countermeasures (e.g., increasing physical security, ensuring physical isolation of the terminal or workstation, increasing personnel security, and/or adding surveillance equipment to ensure that only authorized or trusted personnel are permitted in the vicinity of the terminal or workstation).

- Until NIST completes the ICS project and publishes specific guidance for ICSs, organizations should adjust their ongoing activities aimed at determining compliance with FIPS 200 and SP 800-53 to allow for the types of flexibility that are discussed above. However, it is also reasonable to require ICS owners to develop a multiyear plan to demonstrate how the system owner plans to transition the ICS to a state that is fully compliant with FIPS 200 and SP 800-53, particularly for systems that are planned to be in operation for several more years.

1.2.3 Correspondence of NERC CIPs to NIST Standards and Guidelines

Many of the sector organizations listed in Section 1.4 are working on some aspect of cyber and control system security. At the time this research was conducted, the NERC CIPs were the only available documents that address countermeasures comparable to SP 800-53 for the Electricity Sector. Therefore, this report focuses on comparing the NERC CIPs with SP 800-53.

As discussed in more detail in Section 2.1 of this document, "Cyber Security in the Industrial Process Control Community," and in the appendices, comparing documents produced by different organizations with different frameworks is difficult and error-prone. Inspection of the structure and environments of the NERC CIPs and NIST SP 800-53 makes the following generalizations clear:

- Most requirements in the NERC CIPs correspond to countermeasures in SP 800-53.
- Measures in the NERC CIPs correspond to assessments, which are primarily addressed in SP 800-53A *Guide for Assessing the Security Controls in Federal Information Systems.*
- Compliance in the NERC CIPs corresponds to SP 800-37 *Guide for the Security Certification and Accreditation of Federal Information Systems*.

These rough generalizations characterize the relationship between the types of content within the respective CIP sections relative to different SP publications, without actually commenting on the depth, quality, or rigor pertaining to each. There are exceptions to the generalizations;

for example, the Certification, Accreditation, and Security Assessments (CA) family of countermeasures in SP 800-53 summarizes SP 800-37.

1.2.4 Industrial Control Systems and Critical Infrastructure

ICSs consist of Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), and other industrial control and monitoring systems. ICSs run the nation's mission-critical infrastructure, including such diverse examples as power grids, oil and gas, water treatment facilities, chemical manufacturing facilities, and transportation infrastructure. These networks are increasingly vulnerable to cyber attacks because of the move to standard protocols, interconnections to other networks, and a lack of awareness of security issues that prevailed when some of these systems were deployed. Classic security approaches, in addition, often interfere with the operation of ICSs.

NIST is preparing a *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, SP 800-82, that addresses vulnerabilities, threats, and security countermeasures in the context of developing and deploying cyber security programs. This document will shed additional light on many considerations that are addressed in this report.

Protecting ICSs that support the electric power transmission and distribution systems is a high priority. These systems are an important part of the critical infrastructure for the energy sector and have significant cyber vulnerabilities. While several industry-related efforts are underway to begin developing cyber security standards for ICSs and to harden these potential targets from terrorist attacks, at this time the NERC series of cyber security standards (CIP-002 through CIP-009) are the only published standards for the Electricity Sector.

Federal agencies that own, operate, and maintain ICSs must comply with federal information security standards and guidelines. To date, there has been no serious effort to ensure that the cyber security standards and best practices emerging from the electric power industry are consistent with the federal standards and guidelines being developed by NIST in response to the FISMA.

1.2.5 Background of NERC Critical Infrastructure Protection Standards

Under the Energy Policy Act of 2005, the United States will no longer rely on voluntary compliance with electric industry reliability standards. The law requires that mandatory and enforceable electric reliability standards, approved by the Federal Energy Regulatory Commission (FERC), must be developed. NERC has become FERC's Electric Reliability Organization (ERO), marking a transition of NERC's status. Prior to becoming the ERO, NERC developed the CIP Reliability Standards using a voluntary standards development process accredited by the American National Standards Institute (ANSI). The CIP Reliability Standards were approved by the NERC Board of Trustees in May 2006. FERC staff is conducting a thorough technical review of NERC's existing

voluntary standards, including the CIPs. FERC staff's preliminary assessment[7] of the NERC CIPs has been released for public review and comment. This analysis by MITRE complements and confirms FERC's observations.

1.3 Document Organization

This report becomes increasingly detailed the further one reads (similar to an in-depth newspaper article). Section 1 constitutes the introduction. Section 2 presents the findings and recommendations. Appendix A lists the relevant federal documents. Appendices B and C present detailed analyses of the relationship between the NERC CIPs and SP 800-53, addressing challenges in comparing the documents, requirements and countermeasures, scope, information security policies, and detailed tables. Appendix D contains a glossary and list of acronyms and abbreviations.

1.4 Relevant Professional Organizations

The professional organizations that deal with cyber security standards or control system security standards are grouped below by sector, followed by a list of those that cross-cut several sectors.

- Electric Power
  - NERC North American Electric Reliability Council
  - CIGRE International Council on Large Energy Systems
  - PSRC Power Systems Relay Committee
- Oil and Gas
  - API American Petroleum Institute
  - AGA American Gas Association
  - GTI Gas Technology Institute
- Chemical
  - Chemical Sector Cyber Security Program
- Cross-Cut Organizations
  - ANSI American National Standards Institute
  - IEC International Electrotechnical Commission
  - IEEE Institute of Electrical and Electronic Engineers

[7] *Staff Preliminary Assessment of the North American Electric Reliability Corporation's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection*, RM06-22-000, December 11, 2006. Available at http://www.ferc.gov/industries/electric/indus-act/reliability/12-11-06-cip.pdf

- ISA Instrumentation, Systems, and Automation Society
- ISO International Organization for Standardization

2 Findings and Recommendations

2.1 Cyber Security in the Industrial Process Control Community

The sector organizations identified in Section 1.4 of this document that are concerned with SCADA and ICS have only recently become aware of cyber security issues. Their awareness of the issues, threats, and countermeasures is relatively immature. At the time this research was conducted, the NERC CIPs were the only available standards documents for the Electricity Sector that addressed countermeasures comparable to SP 800-53. The NERC CIP standards (CIP 002-009) are assumed to represent some of the concerns in this sector of the ICS community. MITRE believes that the insights gained comparing the NERC CIP standards to SP 800-53 are useful to NIST and the entire ICS community.

2.1.1 Relationship among NERC CIP and NIST Publications

The NIST publications include a rich foundation for cyber security. Table 2-1 shows the correspondence among the countermeasures in SP 800-53 and other NIST publications, and the requirements in the NERC CIPs. It is not surprising that the NIST publications are overwhelming as compared to the NERC CIPs. Detailed analysis is presented in Appendixes B and C. Many differences in frame of reference, specific the intent of the respective drafters, context, and assumptions tend to cloud the picture. Nonetheless, it is instructive to examine the security concerns addressed.

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-53 Control Family: Access Control – AC	
FIPS 188, Standard Security Labels for Information Transfer, September 1994. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, June 26, 2005. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-19, *Mobile Agent Security*, October 1999. SP 800-28, *Guidelines on Active Content and Mobile Code*, October 2001. SP 800-36, *Guide to Selecting Information Security Products*, October 2003. SP 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002. SP 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002. SP 800-44, *Guidelines on Securing Public Web Servers*, September 2002. SP 800-45, *Guidelines on Electronic Mail Security*, September 2002. SP 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, November 2002.	CIP-003 R1 Cyber Security Policy. CIP-003 R5 Access Control. CIP-004 R4 Access. CIP-005 R1 Electronic Security Perimeter. CIP-005 R2 Electronic Access Controls. CIP-005 R5 Documentation Review and Maintenance. CIP-007 R5 Account Management.

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-57, *Recommendation on Key Management*, August 2005. SP 800-58, *Security Considerations for Voice Over IP Systems*, January 2005. SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, August 2003. SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Systems*, August 2003. SP 800-61, *Computer Security Incident Handling Guide*, January 2004. SP 800-63, Version 1.0.1, *Electronic Authentication Guideline*, September 2004. SP 800-64, *Security Considerations in the Information System Development Life Cycle*, rev 1 June 2004. SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005. SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005. SP 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006. SP 800-73, *Interfaces for Personal Identity Verification*, April 2005. SP 800-76, *Biometric Data Specification for Personal Identity Verification*, February 2006. SP 800-77, *Guide to IPSec VPNs*, December 2005. SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, April 2005. SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006. SP 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, draft September 2006. SP 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005. SP 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*, October 2005 (document updated January 17, 2006). SP 800-95, *Guide to Secure Web Services*, draft August 31, 2006. SP 800-96, *PIV Card/Reader Interoperability Guidelines*, September 2006. SP 800-97, *Guide to IEEE 802.11i: Robust Security Networks*, draft June 5, 2006. SP 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, draft September 26, 2006. SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.	

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-53 Control Family: Awareness and Training – AT	
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998. SP 800-31, *Intrusion Detection Systems (IDS),* November 2001. SP 800-40, *Procedures for Handling Security Patches*, September 2002. SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003. SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.	CIP-003 R1 Cyber Security Policy. CIP-004 R1 Awareness. CIP-004 R2 Training. CIP-004 R2 Training
SP 800-53 Control Family: Audit and Accountability – AU	
FIPS 198, *The Keyed-Hash Message Authentication Code (HMAC),* March 2002. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-42, *Guideline on Network Security Testing*, October 2003. SP 800-44, *Guidelines on Securing Public Web Servers*, September 2002. SP 800-45, *Guidelines on Electronic Mail Security*, September 2002. SP 800-49, *Federal S/MIME V3 Client Profile*, November 2002. SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, June 2005. SP 800-57, *Recommendation on Key Management*, August 2005. SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005. SP 800-72, *Guidelines on PDA Forensics*, November 2004. SP 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005. SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*, November 2006. SP 800-92, *Guide to Computer Security Log Management*, September 2006. SP 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems*, draft August 31, 2006. SP 800-95, *Guide to Secure Web Services*, draft August 31, 2006.	CIP-003 R1 Cyber Security Policy. CIP-005 R3 Monitoring Electronic Access. CIP-005 R5 Documentation Review and Maintenance. CIP-007 R5 Account Management. CIP-007 R6 Security Status Monitoring. CIP-008 R2 Cyber Security Incident Documentation.

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-53 Control Family: Certification, Accreditation, and Security Assessments – CA	
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996 SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998. SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000. SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001. SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002. SP 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems*, May 2004. SP 800-42, *Guideline on Network Security Testing*, October 2003. SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, draft May 4, 2006. SP 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003. SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005. SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-76-1, *Biometric Data Specification for Personal Identity Verification*, draft September 14, 2006. SP 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, July 2005. SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance),* April 2006. SP 800-85B, *PIV Data Model Conformance Test Guidelines*, July 2006.	CIP-003 R1 Cyber Security Policy. CIP-003 R2 Leadership. CIP-003 R4 Information Protection. CIP-005 R2 Electronic Access Controls. CIP-005 R4 Cyber Vulnerability Assessment. CIP-005 R5 Documentation Review and Maintenance. CIP-006 R6 Maintenance and Testing. CIP-007 R1 Test Procedures. CIP-007 R8 Cyber Vulnerability Assessment.

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-53 Control Family: Configuration Management CM	
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-35, *Guide to Information Technology Security Services*, October 2003. SP 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems*, May 2004. SP 800-40, *Procedures for Handling Security Patches*, September 2002. SP 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002. SP 800-44, *Guidelines on Securing Public Web Servers*, September 2002. SP 800-45, *Guidelines on Electronic Mail Security*, September 2002. SP 800-46, *Security for Telecommuting and Broadband Communications*, August 2002. SP 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, November 2002. SP 800-54, *Border Gateway Protocol Security*, draft September 26, 2006. SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005. SP 800-70, *The Security Configuration Checklists Program*, May 2005. SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006. SP 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, draft September 2006. SP 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005. SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.	CIP-002 R3 Critical Cyber Asset Identification. CIP-002 R4 Annual Approval. CIP-003 R1 Cyber Security Policy. CIP-003 R6 Change Control and Configuration Management. CIP-005 R2 Electronic Access Controls. CIP-005 R5 Documentation Review and Maintenance. CIP-007 R1 Test Procedures. CIP-007 R2 Ports and Services. CIP-007 R3 Security Patch Management. CIP-007 R9 Documentation Review and Maintenance.

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-53 Control Family: Contingency Planning – CP	
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-21-1, *Guideline for Implementing Cryptography in the Federal Government*, Second edition, December 2005. SP 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000. SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000. SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002. SP 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002. SP 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002. SP 800-44, *Guidelines on Securing Public Web Servers*, September 2002. SP 800-45, *Guidelines on Electronic Mail Security*, September 2002. SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2006. SP 800-57, *Recommendation on Key Management*, August 2005. SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006. SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006. SP 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005. SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006. SP 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, draft September 26, 2006.	CIP-009 R1 Recovery Plans. CIP-009 R2 Exercises. CIP-009 R3 Change Control. CIP-009 R4 Backup and Restore. CIP-009 R5 Testing Backup Media.

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-53 Control Family: Identification and Authentication – IA	
FIPS 140-2, *Security requirements for Cryptographic Modules*, May 2001. FIPS 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 1994. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, June 26, 2005. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000. SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000. SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001. SP 800-33, *Underlying Technical Models for Information Technology Security*, December 2001. SP 800-44, *Guidelines on Securing Public Web Servers*, September 2002. SP 800-45, *Guidelines on Electronic Mail Security*, September 2002. SP 800-46, *Security for Telecommuting and Broadband Communications*, August 2002. SP 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, November 2002. SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, June 2005. SP 800-63, Version 1.0.1, *Electronic Authentication Guideline*, September 2004. SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005. SP 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006. SP 800-72, *Guidelines on PDA Forensics*, November 2004. SP 800-73, *Interfaces for Personal Identity Verification*, April 2005. SP 800-76-1, *Biometric Data Specification for Personal Identity Verification*, draft September 14, 2006. SP 800-77, *Guide to IPSec VPNs*, December 2005. SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, April 2005.	CIP-003 R1 Cyber Security Policy. CIP-005 R2 Electronic Access Controls. CIP-007 R5 Account Management

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006. SP 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*, October 2005 (document updated January 17, 2006). SP 800-96, *PIV Card/Reader Interoperability Guidelines*, September 2006. SP 800-97, *Guide to IEEE 802.11i: Robust Security Networks*, draft June 5, 2006. SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.	
SP 800-53 Control Family: Incident Response – IR	
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-61, *Computer Security Incident Handling Guide*, January 2004. SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006. SP 800-92, *Guide to Computer Security Log Management*, September 2006. SP 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems*, draft August 31, 2006. SP 800-101, *Guidelines on Cell Phone Forensics*, draft August 31, 2006.	CIP-008 R1 Cyber Security Incident Response Plan.
SP 800-53 Control Family: Maintenance – MA	
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002. SP 800-77, *Guide to IPSec VPNs*, December 2005. SP 800-88, *Guidelines for Media Sanitization*, September 2006. SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.	CIP-003 R1 Cyber Security Policy. CIP-006 R6 Maintenance and Testing.

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-53 Control Family: Media Protection – MP	
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000. SP 800-36, *Guide to Selecting Information Security Products*, October 2003. SP 800-57, *Recommendation on Key Management*, August 2005. SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-72, *Guidelines on PDA Forensics*, November 2004. SP 800-88, *Guidelines for Media Sanitization*, September 2006. SP 800-92, *Guide to Computer Security Log Management*, September 2006. SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.	CIP-003 R1 Cyber Security Policy. CIP-007 R7 Disposal or Redeployment.
SP 800-53 Control Family: Physical and Environmental Protection – PE	
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000. SP 800-58, *Security Considerations for Voice Over IP Systems*, January 2005. SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005. SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-73, *Interfaces for Personal Identity Verification*, April 2005. SP 800-76-1, *Biometric Data Specification for Personal Identity Verification*, draft September 14, 2006. SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, April 2005. SP 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, draft September 2006. SP 800-96, *PIV Card/Reader Interoperability Guidelines*, September 2006. SP 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, draft September 26, 2006. SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.	CIP-003 R1 Cyber Security Policy. CIP-006 R1 Physical Security Plan. CIP-006 R2 Physical Access Controls. CIP-006 R3 Monitoring Physical Access. CIP-006 R4 Logging Physical Access. CIP-006 R5 Access Log Retention.

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-53 Control Family: Planning – PL	
FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, June 26, 2005. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-18, *Guide for Developing Security Plans for Information Technology Systems,* December 1998. SP 800-19, *Mobile Agent Security*, October 1999. SP 800-21-1, *Guideline for Implementing Cryptography in the Federal Government*, Second edition, December 2005. SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000. SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001. SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security),* Revision A June 2004. SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002. SP 800-31, *Intrusion Detection Systems (IDS),* November 2001. SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001. SP 800-33, *Underlying Technical Models for Information Technology Security*, December 2001. SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002. SP 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems*, May 2004. SP 800-40, *Procedures for Handling Security Patches*, September 2002. SP 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002. SP 800-42, *Guideline on Network Security Testing*, October 2003. SP 800-44, *Guidelines on Securing Public Web Servers*, September 2002. SP 800-45, *Guidelines on Electronic Mail Security*, September 2002. SP 800-46, *Security for Telecommuting and Broadband Communications*, August 2002. SP 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, November 2002.	CIP-003 R1 Cyber Security Policy. CIP-003 R3 Exceptions. CIP-007 R1 Test Procedures.

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-57, *Recommendation on Key Management*, August 2005. SP 800-58, *Security Considerations for Voice Over IP Systems*, January 2005. SP 800-64, *Security Considerations in the Information System Development Life Cycle*, rev 1 June 2004. SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005. SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006. SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*, November 2006. SP 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, draft September 26, 2006. SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.	
SP 800-53 Control Family: Personnel Security – PS	
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.	CIP-004 R3 Personnel Risk Assessment. CIP-004 R4 Access. CIP-007 R5 Account Management.

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-53 Control Family: Risk Assessment – RA	
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-19, *Mobile Agent Security*, October 1999. SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000. SP 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000. SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000. SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001. SP 800-28, *Guidelines on Active Content and Mobile Code*, October 2001. SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002. SP 800-31, *Intrusion Detection Systems (IDS),* November 2001. SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001. SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002. SP 800-36, *Guide to Selecting Information Security Products*, October 2003. SP 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems*, May 2004. SP 800-40, *Procedures for Handling Security Patches,* September 2002. SP 800-42, *Guideline on Network Security Testing*, October 2003. SP 800-44, *Guidelines on Securing Public Web Servers*, September 2002. SP 800-45, *Guidelines on Electronic Mail Security*, September 2002. SP 800-46, *Security for Telecommuting and Broadband Communications*, August 2002. SP 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, November 2002. SP 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002. SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, draft May 4, 2006. SP 800-54, *Border Gateway Protocol Security*, draft September 26, 2006.	CIP-002 R1 Critical Asset Identification Method. CIP-003 R4 Information Protection. CIP-005 R4 Cyber Vulnerability Assessment. CIP-005 R5 Documentation Review and Maintenance. CIP-007 R3 Security Patch Management CIP-007 R8 Cyber Vulnerability Assessment.

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, August 2003. SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security System*, August 2003. SP 800-63, Version 1.0.1, *Electronic Authentication Guideline*, September 2004. SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005. SP 800-66, An *Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, draft September 2006. SP 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005. SP 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, draft September 26, 2006. SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.	

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-53 Control Family: System and Services Acquisition – SA	
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-21-1, *Guideline for Implementing Cryptography in the Federal Government*, Second edition December 2005. SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000. SP 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security),* Revision A June 2004. SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002. SP 800-31, *Intrusion Detection Systems (IDS),* November 2001. SP 800-33, *Underlying Technical Models for Information Technology Security*, December 2001. SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002. SP 800-35, *Guide to Information Technology Security Services*, October 2003. SP 800-36, *Guide to Selecting Information Security Products*, October 2003. SP 800-64, *Security Considerations in the Information System Development Life Cycl*e, rev 1 June 2004. SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005. SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-76-1, *Biometric Data Specification for Personal Identity Verification*, draft September 14, 2006. SP 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005. SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance),* April 2006. SP 800-85B, *PIV Data Model Conformance Test Guidelines*, July 2006. SP 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems*, draft August 31, 2006. SP 800-97, *Guide to IEEE 802.11i: Robust Security Networks*, draft June 5, 2006. SP 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, draft September 26, 2006. SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.	CIP-003 R1 Cyber Security Policy.

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-53 Control Family: System and Communications Protection – SC	
FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 2001. FIPS 180-2, *Secure Hash Standard (SHS),* August 2002, change notice February 2004. FIPS 186-2, *Digital Signature Standard (DSS),* January 2000. FIPS 198, *The Keyed-Hash Message Authentication Code (HMAC),* March 2002. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006. FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* June 26, 2005. SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology H*andbook, October 1995. SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996. SP 800-15, *Minimum Interoperability Specification for PKI Components (MISPC),* Version 1 September 1997. SP 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, February 1998. SP 800-19, *Mobile Agent Security*, October 1999. SP 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TDEA): Requirements and Procedures*, October 1999, revised April 2000. SP 800-21-1, *Guideline for Implementing Cryptography in the Federal Government*, Second edition December 2005. SP 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, October 2000, revised May 15, 2001. SP 800-28, *Guidelines on Active Content and Mobile Code*, October 2001. SP 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001. SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001. SP 800-36, *Guide to Selecting Information Security Products*, October 2003. SP 800-38A, *Recommendation for Block Cipher Modes of Operation — Methods and Techniques*, December 2001. SP 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005. SP 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, May 2004. SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication*, draft April 20, 2006. SP 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002. SP 800-44, *Guidelines on Securing Public Web Servers*, September 2002.	CIP-003 R1 Cyber Security Policy. CIP-005 R1 Electronic Security Perimeter. CIP-005 R2 Electronic Access Controls. CIP-005 R5 Documentation Review and Maintenance.

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-45, *Guidelines on Electronic Mail Security*, September 2002. SP 800-46, *Security for Telecommuting and Broadband Communications*, August 2002. SP 800-49, *Federal S/MIME V3 Client Profile*, November 2002. SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, June 2005. SP 800-54, *Border Gateway Protocol Security*, draft September 26, 2006. SP 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003. SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2006. SP 800-57, *Recommendation on Key Management*, August 2005. SP 800-58, *Security Considerations for Voice Over IP Systems*, January 2005. SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005. SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2004. SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005. SP 800-70, *The Security Configuration Checklists Program*, May 2005. SP 800-73, *Interfaces for Personal Identity Verification*, April 2005. SP 800-77, *Guide to IPSec VPNs*, December 2005. SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, April 2005. SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006. SP 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, draft September 2006. SP 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005. SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2006. SP 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems*, draft August 31, 2006. SP 800-95, *Guide to Secure Web Services*, draft August 31, 2006. SP 800-97, *Guide to IEEE 802.11i: Robust Security Networks*, draft June 5, 2006. SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.	

Table 2-1. Where Security Concerns are Addressed

NIST Publications (other than SP 800-53)	Applicable NERC CIP Requirement
SP 800-53 Control Family: System and Information Integrity – SI	
FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006. *SP 800-12, An Introduction to Computer Security: the National Institute of Standards and Technology Handbook, October 1995.* *SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996.* *SP 800-19, Mobile Agent Security, October 1999.* *SP 800-28, Guidelines on Active Content and Mobile Code, October 2001.* *SP 800-30, Risk Management Guide for Information Technology Systems, January 2002.* *SP 800-31, Intrusion Detection Systems (IDS), November 2001.* *SP 800-36, Guide to Selecting Information Security Products, October 2003.* *SP 800-40, Procedures for Handling Security Patches, September 2002.* *SP 800-42, Guideline on Network Security Testing, October 2003.* *SP 800-43, Systems Administration Guidance for Windows 2000 Professional, November 2002.* *SP 800-44, Guidelines on Securing Public Web Servers, September 2002.* *SP 800-45, Guidelines on Electronic Mail Security, September 2002.* *SP 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme, September 2002.* *SP 800-57, Recommendation on Key Management, August 2005* *SP 800-61, Computer Security Incident Handling Guide, January 2004.* *SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, March 2005.* *SP 800-69, Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist, September 2006.* *SP 800-83, Guide to Malware Incident Prevention and Handling, November 2005.* *SP 800-85A, PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance), April 2006.* *SP 800-85B, PIV Data Model Conformance Test Guidelines, July 2006.* *SP 800-94, Guide to Intrusion Detection and Prevention (IDP) Systems, draft August 31, 2006.* *SP 800-100, Information Security Handbook: A Guide for Managers*, October 2006.	CIP-003 R1 Cyber Security Policy. CIP-007 R3 Security Patch Management. CIP-007 R4 Malicious Software Prevention. CIP-007 R6 Security Status Monitoring.

2.1.2 Comparing Documents from Different Organization Frameworks

NIST issues standards and guidelines that are directed to non-national security information and information systems belonging to, or operated for, federal government agencies. These agencies issue within their own systems orders, instructions, manuals, and standards that interpret and elaborate upon the various government publications' applicability to their agency. Similar models apply to regulatory agencies and the private sector.

A list, or catalog, of relevant federal government documents is presented in Appendix A of this document. Examination of this set of documents shows a patchwork "quilt" of multiple authorities and overlapping domains. Identical or related topics are often addressed in multiple documents. Creating a taxonomy, or organization table, of the topics would be extremely difficult. Consistency is impossible because the documents change asynchronously.

MITRE expects each organization (and its documents) to continue to have unique viewpoints, history, context, etc. The grouping of topics will undoubtedly differ from the federal model. A deliberate, targeted effort is required for two organizations to follow the same outline or structure. Any comparison between documents in two sets, such as NERC CIPs and SP 800-53, will not be one-to-one.

2.1.3 Context of NIST Standards and Guidelines Addressing Cyber Security

As discussed in more detail in the appendices, comparing documents produced by different organizations with different frameworks is difficult and error-prone. This section highlights the context of SP 800-53 for readers unfamiliar with the history and practice of cyber security in the federal government.

A number of laws and presidential directives address cyber security, including:

- Critical Infrastructure Identification, Prioritization, and Protection Presidential Directive No. 7 (HSPD-7), December 17, 2003
- National Strategy to Secure Cyberspace, February 2003
- Management of Federal Information Resources, Office of Management and Budget (OMB) Circular A-130, Revised, Transmittal Memorandum No. 4, November 28, 2000
- Federal Information Security Management Act of 2002 (FISMA)
- Homeland Security Act of 2002
- Sarbanes-Oxley Act of 2002
- Patriot Act of 2001
- Digital Privacy Act of 2000
- Electronic Communications Privacy Act of 1986, 2000

- Gramm-Leach-Bliley Act of 1999
- Critical Infrastructure Protection, Presidential Decision Directive (PDD) No. 63, May 22, 1998
- Health Insurance Portability and Accountability Act (HIPAA), 1996
- National Infrastructure Protection Act of 1996
- Computer Security Act of 1987
- Computer Fraud and Abuse Act of 1986
- Computer Crime Control Act 1984
- Privacy Act of 1974

Responsibilities for non-national security systems are assigned to multiple agencies, including:

- Department of Health and Human Services (HHS)
- Department of Homeland Security (DHS)
- Department of Justice (DoJ)
- Federal Bureau of Investigation (FBI)
- General Services Administration (GSA)
- National Institute of Standards and Technology (NIST)
- Office of Management and Budget (OMB)
- Security Exchange Commission (SEC)

2.1.4 When Multiple Paradigms Apply

Some organizations may be required to conform to overlapping standards and guidelines. Trying to conform to multiple requirements is difficult. For example, at present federal agencies that own or operate electric energy transmission and distribution systems must follow SP 800-53, and they may voluntarily choose to follow the NERC CIPs.

This comparison of the NERC CIPs and SP 800-53 is being performed on those parts of the two documents that have a direct correspondence as determined by expert judgment. Gradations in the degree of correspondence are recorded in a table using code numbers as presented in Appendix B. Representative findings include the following:

- NERC requirements include management responsibilities that are outside the scope of SP 800-53.
- Management is given much greater latitude in the NERC CIPs for limiting the scope of concern and accepting risk.
- The NERC requirements vary widely in generality and specificity as compared to SP 800-53 controls.
- Requirements and controls are essentially equivalent.
- NERC requirements address a subset of the Moderate Baseline set of controls in SP 800-53.
  - This subset is inadequate for protecting critical national infrastructure.
  - The Moderate Baseline is inadequate for all electric energy systems when the impact of regional and national power outages is considered.

Vocabulary differences exacerbate the difficulty of comparison. As mentioned previously, SP 800-53 prefers the term "control," which it equates to "safeguards" and "countermeasures." The NERC CIP use "measures" in the sense of metrics or evidence that demonstrate compliance with the standard. While that usage does not corresponds to SP 800-53, and is therefore excluded from this report, "measure" can be confused with "countermeasure."

Analysis of the organization and structure of the NERC CIPs identified how the section of each NERC standard titled "Requirements" corresponds to the security countermeasures specified in SP 800-53. The SP 800-53 introduction states: "Security controls (countermeasures) are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information." In other words, countermeasures are what the organization must do.

As shown in Table 2-1, parts of the NERC CIPs correspond to elements in other federal publications. For example, the NERC CIPs identify "measures [(metrics) that] will be used to demonstrate compliance with the requirements." The corresponding concept in federal publications occurs in SP 800-53A *Guide for Assessing the Security Controls in Federal Information System*, which states: "Once employed within an information system, security controls (countermeasures) must be assessed to determine the extent to which the controls (countermeasures) are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system."

NIST addresses "certification" and "accreditation" in great detail in SP 800-26 *Security Self-Assessment Guide for Information Technology Systems* and SP 800-37 *Guide for Security Certification and Accreditation of Federal Information Systems* with the following meanings:

- Certification – A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Accreditation – The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

The NERC CIPs are quite brief in comparison to SP 800-26 and SP 800-37. They appear to use "management approval" synonymously with "accreditation." "Certification" per se is not mentioned, but "self-certification" is used without definition. The NERC CIPs all contain a "compliance" section in the organization structure, but the term "compliance" is not defined. MITRE infers that the compliance sections in the NERC CIPs correspond with SP 800-26 and SP 800-37.

The "compliance" sections contain subheadings for "compliance monitoring process" and "levels of non-compliance." The treatment of "compliance" is rather sketchy and does not support an objective determination of whether requirements are being met. The NERC CIP requirements are less precise than SP 800-26 and SP 800-37. There is an inherent conflict of interest in giving company officials the role of approving operations and determining compliance that the FISMA paradigm avoids by separation of duties.

2.1.5 Recommendation

Because the scope of the NERC CIPs is a subset of the FISMA scope, federal agencies should adhere to the FISMA scope. If an organization required to conform to SP 800-53 also wishes to conform to the NERC CIPs, the organization should document its activities in a way to meet both paradigms.

There is no reason that the electric power sector should implement cyber security controls and counter measures that are inferior to the federal government's. MITRE believes that the relevant NIST publications, including FIPS 199, FIPS 200, and SP 800-53, constitute a comprehensive and coherent basis for cyber security in the electric power sector. MITRE recommends that NIST and FERC work together to evolve these publications to better address the electric power sector, including both public and private entities. Specifically, NIST and FERC should work together to develop an interpretation of SP 800-53 that is applicable to both public and private entities in the electric power sector.

2.2 Information Security Policy

2.2.1 Finding

A basic premise of the FISMA paradigm is that an organization must have information security policies. It is not possible to differentiate acceptable and unacceptable behavior and conditions without a policy. Enumerating a set of procedures is insufficient.

Threat and business environments are continually changing, and policies must be flexible to anticipate such changes. Organizations must manage information security policies so that they can evolve with the changing legal, regulatory, and corporate governance requirements. Organizations must enforce their policies consistently and provide proof of conformance and remediation procedures. Although the NERC CIPs do not require organizations to create policies at the same level as SP 800-53, a notation was made that NERC was attempting to address policy. MITRE has inferred that the group that drafted the NERC CIPs thought that its specifications constituted sufficient policy.

2.2.2 Recommendation

Organizations should create and maintain information security policies that are germane to their missions and objectives. These policies should be flexible, enforceable, and support conformance reporting and remediation.

2.3 Identifying Critical Information Technology

This section addresses issues and differences between the FISMA and NERC CIP paradigms for identifying critical IT.

2.3.1 FISMA Paradigm

FIPS 200 mandates that federal organizations adhere to the security controls in SP 800-53. FIPS 199 establishes standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency. The security categories are based on the potential impact on an organization should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

FIPS 199 requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. SP 800-53 control RA-2 Security Categorization clarifies the scope guidance in FIPS 199: "The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives (HSPD), potential national-level impacts in categorizing the information system."

FIPS 200 specifies minimum security requirements for federal information and information systems. Federal agencies must meet the minimum security requirements as defined in FIPS 200 by using

the security controls specified in SP 800-53, *Recommended Security Controls for Federal Information Systems*, as amended.

2.3.2 NERC CIP Paradigm

The NERC CIPs provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. CIP-002 requires the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System to be identified and documented. These Critical Assets are to be identified through the application of a risk-based assessment. The applicable definitions from the NERC Reliability Standards Glossary of Terms are:

- Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.
- Cyber Assets: Programmable electronic devices and communication networks, including hardware, software, and data.
- Critical Cyber Assets: Cyber Assets essential to the reliable operation of Critical Assets.

The procedure for applying the NERC CIPs is to first identify Critical Assets that support the reliable operation of the Bulk Electric System, then identify the Critical Cyber Assets that are essential to the Critical Assets.

2.3.3 Comparison

The IT systems addressed by the NERC CIP paradigm are a subset of those addressed by the FISMA paradigm. Also, the objectives used for determining the importance of the IT systems addressed are narrower in the NERC CIP paradigm than they are in the FISMA paradigm. A high-level comparison of the two paradigms shows:

- The FISMA paradigm is concerned with the potential impact on an organization should certain events occur that jeopardize the information and information systems needed by the organization to:
  - Accomplish its assigned mission
  - Protect its assets
  - Fulfill its legal responsibilities
  - Maintain its day-to-day functions
  - Protect individuals
  - Reduce potential national-level impacts
- The NERC CIPs are concerned with the reliability and operability of the Bulk Electric System, excluding:
  - Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission

– Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters

Be it through direct connectivity or geospatial proximity, most critical infrastructure systems interact. These interactions often create complex relationships, dependencies, and interdependencies that cross infrastructure boundaries.[8] One example is an isolated electrical substation that supplies electric power to water and sewerage pumps[9]. While a prolonged outage of the substation may have no effect on the Bulk Electric System, a prolonged outage of water and sewerage pumps could have severe impact on these other critical infrastructures.

FIPS 199 is concerned with the potential impact on an organization, other organizations connected to it, and (in accordance with the Patriot Act and HSPDs) potential national-level impacts, should events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. This is a broad scope that the organization is left to interpret. It is obviously much broader than the scope of the NERC CIPs, but without further guidance it is not possible to identify its boundaries.

2.3.4 Recommendations

- Because the scope of the NERC CIPs is a subset of the FISMA scope, federal agencies should adhere to the FISMA scope.
- NIST and FERC should work together to develop an interpretation of SP 800-53 that is applicable to both public and private entities in the electric power sector.

---

[8] Pederson, P., *et al.*, *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*, Idaho National Laboratory report INL/EXT-06-11464, August 2006.

[9] David. Norton, Entergy, private communication.

Appendix A Relevant Federal Government Documents

The following federal government documents help define the cyber security environment. It is important to note that many independent authorities are creating and revising these documents asynchronously. Regulations and guidance may not always be consistent. This list is not exhaustive. Other federal laws, regulations, and guidance not listed here may apply. Many organizations are governed by legislation that specifically applies to that organization. In addition, organizations tend to produce interpretations of external regulations and other publications for the conduct of their activities and the guidance of their employees and contractors.

A.1 Federal Laws and Regulations

- Public Law 107-347, Federal Information Security Management Act of 2002, December 17, 2002.
- Public Law 107-296, Critical Information Infrastructure Act of 2002.
- Public Law 104-106, Clinger-Cohen Act of 1996.
- Public Law 99-474, The Computer Fraud and Abuse Act.
- 5 United States Code (U.S.C.) Section 552, "The Privacy Act of 1974."
- 44 U.S.C. Chapter 35, "Coordination of Federal Information Policy."
- United States Code of Federal Regulations (CFR) 29, Department of Homeland Security, "Procedures for Handling Critical Infrastructure Information."

A.2 Executive Orders

- Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions, April 3, 1984.
- Executive Order 13011, Federal Information Technology, July 16, 1996.
- Executive Order 13231, Critical Infrastructure Protection in the Information Age, October 16, 2001.
- PDD-63, Protecting America's Critical Infrastructures, May 22, 1998.
- Homeland Security Presidential Directive-3 (HSPD-3), Homeland Security Advisory System, March 11, 2002.

A.3 Office of Management and Budget

- OMB Circular Number A-130, *Management of Federal Information Resources*, February 8, 1996.
- OMB Circular Number A-123, *Management Accountability and Control*, revised June 21, 1999.
- OMB Circular A-11, *Preparation, Submission, Execution of Budgets*, July 16, 2004.
- OMB Memorandum M-00-10, *Procedures and Guidelines on Implementing the Government Paperwork Elimination Act*, April 25, 2002.
- PDD 12, *Security Awareness and Reporting of Foreign Contacts*, August 5, 1993.
- OMB Guide, *Evaluating Information Technology Investments*; http://www.whitehouse.gov/omb/inforeg/infotech.html, February 2, 2006

A.4 Department of Homeland Security (DHS)

- Homeland Security Presidential Directive (HSPD), DHS Policy Directive 3, *Homeland Security Advisory System*, March 11, 2002.
- HSPD, DHS Policy Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- HSPD, DHS Policy Directive 12, *Common Identification Standard for Federal Employees and Contractors*, August 24, 2004.

A.5 Department of Commerce (DOC)

- FIPS 140-2, *Security requirements for Cryptographic Modules*, May 2001.
- FIPS 180-2, *Secure Hash Standard (SHS)*, August 2002, change notice February 2004.
- FIPS 186-2, *Digital Signature Standard (DSS)*, January 2000.
- FIPS 188, *Standard Security Labels for Information Transfer*, September 1994.
- FIPS 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 1994
- FIPS 198, *The Keyed-Hash Message Authentication Code (HMAC)*, March 2002.
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

- FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, February 25, 2005.
- FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001.
- SP 800-12, *An Introduction to Computer Security: the National Institute of Standards and Technology Handbook*, October 1995.
- SP 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, October 1995.
- SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.
- SP 800-15, *Minimum Interoperability Specification for PKI Components (MISPC), Version 1*, September 1997.
- SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.
- SP 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, February 1998.
- SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.
- SP 800-19, *Mobile Agent Security*, October 1999.
- SP 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TDEA): Requirements and Procedures*, October 1999, revised April 2000.
- SP 800-21-1, *Guideline for Implementing Cryptography in the Federal Government, Second edition*, December 2005.
- SP 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, October 2000, revised: May 15, 2001.
- SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.
- SP 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000.
- SP 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000.
- SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.
- SP 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A June 2004.

- SP 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.
- SP 800-30, *Risk Management Guide for Information Technology Systems*, January 2002.
- SP 800-31, *Intrusion Detection Systems (IDS)*, November 2001.
- SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.
- SP 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.
- SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.
- SP 800-35, *Guide to Information Technology Security Services*, October 2003.
- SP 800-36, *Guide to Selecting Information Security Products*, October 2003.
- SP 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems*, May 2004.
- SP 800-38A, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*, December 2001.
- SP 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005.
- SP 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, May 2004.
- SP 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication*, draft April 20, 2006.
- SP 800-40, *Procedures for Handling Security Patches*, September 2002.
- SP 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002.
- SP 800-42, *Guideline on Network Security Testing*, October 2003.
- SP 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002.
- SP 800-44, *Guidelines on Securing Public Web Servers*, September 2002.
- NIST SP 800-45, *Guidelines on Electronic Mail Security*, September 2002.
- SP 800-46, *Security for Telecommuting and Broadband Communications*, August 2002.

- SP 800-47, *Security Guide for Interconnecting Information Technology Systems,* September 2002.
- SP 800-48, *Wireless Network Security 802.11, Bluetooth and Handheld Devices,* November 2002.
- SP 800-49, *Federal S/MIME V3 Client Profile*, November 2002.
- SP 800-50, *Building an Information Technology Security Awareness and Training Program,* October 2003.
- SP 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme,* September 2002.
- SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations,* June 2005.
- SP 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.
- SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems,* draft May 4, 2006.
- SP 800-54, *Border Gateway Protocol Security*, draft September 26, 2006.
- SP 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.
- SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography,* March 2006.
- SP 800-57, *Recommendation on Key Management,* August 2005.
- SP 800-58, *Security Considerations for Voice Over IP Systems*, January 2005.
- SP 800-59, *Guidelines for Identifying an Information System as a National Security System,* August 2003.
- SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security System,* August 2003.
- SP 800-61, *Computer Security Incident Handling Guide*, January 2004.
- SP 800-63, Version 1.0.1, *Electronic Authentication Guideline*, September 2004.
- SP 800-64, *Security Considerations in the Information System Development Life Cycle,* rev 1 June 2004.
- SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process,* January 2005.
- SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005.

- SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2004.
- SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005.
- SP 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006.
- SP 800-70, *The NIST Security Configuration Checklists Program*, May 2005.
- SP 800-72, *Guidelines on PDA Forensics*, November 2004.
- SP 800-73, *Interfaces for Personal Identity Verification*, April 2005.
- SP 800-76-1, *Biometric Data Specification for Personal Identity Verification*, draft September 14, 2006.
- SP 800-77, *Guide to IPSec VPNs*, December 2005.
- SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, April 2005.
- SP 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, July 2005.
- SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006.
- SP 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, draft September 2006.
- SP 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005.
- SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.
- SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance)*, April 2006.
- SP 800-85B, *PIV Data Model Conformance Test Guidelines*, July 2006.
- SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006.
- SP 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*, October 2005 (document updated January 17, 2006).
- SP 800-88, *Guidelines for Media Sanitization*, September 2006.
- SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*, November 2006.

- SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2006.
- SP 800-92, *Guide to Computer Security Log Management*, September 2006.
- SP 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems*, draft August 31, 2006.
- SP 800-95, *Guide to Secure Web Services*, draft August 31, 2006.
- SP 800-96, *PIV Card/Reader Interoperability Guidelines*, September 2006.
- SP 800-97, *Guide to IEEE 802.11i: Robust Security Networks*, draft June 5, 2006.
- SP 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, draft September 26, 2006.
- SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.
- SP 800-101, *Guidelines on Cell Phone Forensics*, draft August 31, 2006.

A.6 Government Accountability Office (GAO)

- GAO/AIMD-94-115, *Executive Guide: Improving Mission Performance through Strategic Information Management and Technology*, May 1994.
- GAO/AIMD-10.1.13, *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making*, February 1997.
- GAO/AIMD-12.19.6, *Federal Information System Controls Audit Manual*, January 1999.
- GAO-04-394G, *Information Technology Investment Management – A Framework for Assessing and Improving Process Maturity*, March 2004.

A.7 Federal CIO Council

- *Federal Information Technology Security Assessment Framework*, November 2000.

A.8 Other Sources

- Committee on National Security Systems (CNSS), National Security Telecommunications and Information Systems Security Instruction (NSTISSI) Number 4009, *National Information Systems Security Glossary*, September 2000.
- Federal Energy Regulatory Commission, *Staff Preliminary Assessment of the North American Electric Reliability Corporation's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection*, RM06-22-000, December 11, 2006.

Appendix B Relationship between the NERC CIPs and SP 800-53

This appendix presents several tables summarizing the relationship between the NERC CIP and SP 800-53. Additional detail is presented in Appendix C of this document.

B.1 Challenges in Comparing Documents

An examination of the list of relevant federal government documents presented in Appendix A shows a patchwork of multiple authorities and overlapping domains. Identical or related topics are often addressed in multiple documents. Creating a taxonomy, or organization table, of the topics would be extremely difficult. Consistency is impossible because the documents change asynchronously.

Some organizations may need to conform to overlapping standards and guidelines. Trying to conform to multiple requirements is confusing and difficult. When there is conflict between standards, the difficulty escalates. For example, federal agencies that own or operate electric energy transmission and distribution systems come under SP 800-53 and might also want to conform to the NERC CIPs.

This comparison of the NERC CIPs and SP 800-53 is being performed on those parts of the two sets of documents that directly correspond to each other, as determined by expert judgment. Echoing the explanations preceding the security control mappings in Appendix G of SP 800-53, which show the relationship of the SP 800-53 security controls to other standards and control sets, please note that the mapping table in this appendix provides a general indication of SP 800-53 security control coverage with respect to the NERC CIP standards. The security control mappings are not exhaustive, and they are based on a broad interpretation and general understanding of the control sets being compared. The mappings have been created by a two-way search that used the primary security topic identified in each of the SP 800-53 security controls/NERC CIP requirements and searching for a similar security topic in the NERC CIP requirements/SP 800-53 security controls. Security controls with similar functional meaning are included in the mapping table.

The granularity and level of abstraction of the security control sets being compared is not always the same. This difference in granularity and level of abstraction makes the security control mappings less precise in some instances. Therefore, the mappings should not be used as a "checklist" for the express purpose of comparing security capabilities or security implementations across information systems assessed against different control sets. MITRE recommends that NIST develop supplemental guidance for organizations that wish to comply with both SP 800-53 and the NERC CIPS.

The standards and guidelines issued by NIST are directed to non-national security information and information systems that belong to, or are operated for, federal government agencies. These agencies issue their own systems orders, instructions, manuals, and standards that interpret and elaborate upon the various government publications' applicability to their agency. Similar models apply to regulatory agencies and the private sector. For example, NERC could

choose to relate more closely to SP 800-53 by recasting its requirements as interpretations of the SP 800-53 controls.

MITRE expects each organization (and its documents) to continue to have unique viewpoints, history, context, etc. Organizations may group their topics differently from the federal model. A deliberate, targeted effort is required for two organizations to follow the same structure. Any comparison between documents created by two different organizations, such as NERC CIPs and SP 800-53, will not be one-to-one. There are topics in the NERC CIPs that have no corresponding topics in SP 800-53, and vice versa.

B.2 Requirements and Controls

This report focuses on common themes between NIST SP 800-53 and the NERC CIPs. The topics addressed in the NERC CIPs that correspond to other federal publications, but not to SP 800-53, are not addressed. The breadth of federal publications allows organizations to focus a document on a specific subset of the general problem of cyber security. One way of categorizing the publications itemized in Appendix A is by the questions they answer and the topics they address, such as:

- Management of information and information systems security
- Protecting critical information infrastructure
- Protecting privacy in information systems
- Determining risk, threat, and vulnerability
- Information systems security plans, policies, procedures, and operations
- Measuring and assessing controls, plans, policies, procedures, and operations
- Controls and countermeasures
- Awareness and training
- Contingency planning

B.3 Scope

SP 800-53 addresses the selection and employment of appropriate security controls for an information system. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. In other words, controls are what the organization must do. SP 800-53 provides guidance for addressing several important issues:

- Security controls needed to adequately protect the information systems that support an organization's operations and assets in order for the organization to:
  - Accomplish its assigned mission
  - Protect its assets
  - Fulfill its legal responsibilities

  - Maintain its day-to-day functions
  - Protect individuals
- Whether the selected security controls have been implemented, or there is a realistic plan to implement them
- The appropriate level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented, are (or will be) effective in their application

NERC was designated the Sector Coordinator for the Electricity Sector under PDD-63, "Protecting America's Critical Infrastructures," that officially identified electricity as a critical infrastructure. PDD-63, and the later HSPD-3, calls for a framework for cooperation within individual infrastructure sectors and with government for the vital mission of protecting critical infrastructures. NERC, as the Sector Coordinator, has the responsibility to:

- Assess sector vulnerabilities
- Develop a plan to reduce electric system vulnerabilities
- Propose a system for identifying and averting attacks
- Develop a plan to alert Electricity Sector participants and appropriate government agencies that an attack is imminent or in progress
- Assist in reconstituting minimum essential electric system capabilities in the aftermath of an attack

The NERC CIPs were developed in this context to apply to electric infrastructure systems, including:

- Balancing authorities
- Generator owners and operators
- Interchange authorities
- Load-serving entities
- Offices of NERC
- Regional reliability organizations
- Reliability coordinators
- Transmission owners and operators

The following were excluded from coverage:

- Communication networks and communications

- Facilities regulated by the U.S. Nuclear Regulatory Commission and the Canadian Nuclear Safety Commission
- Links between discrete Electronic Security Perimeters

B.4 Tables of Content

It is instructive to compare the NERC CIPs and SP 800-53 at the level of their tables of contents. Table B-1 tabulates the requirements from the NERC CIPs, and Table B-2 is from SP 800-53.

Table B-1. CIP Cyber Security Standards Requirements

System Control Requirement
Standard CIP-002-1 — Critical Cyber Assets
R1. Critical Asset Identification Method
R2. Critical Asset Identification
R3. Critical Cyber Asset Identification
R4. Annual Approval
Standard CIP-003-1 — Security Management Controls
R1. Cyber Security Policy
R2. Leadership
R3. Exceptions
R4. Information Protection
R5. Access Control
R6. Change Control and Configuration Management
Standard CIP-004-1 — Personnel & Training
R1. Awareness
R2. Training
R3. Personnel Risk Assessment
R4. Access
Standard CIP-005-1 — Electronic Security
R1. Electronic Security Perimeter
R2. Electronic Access Controls
R3. Monitoring Electronic Access
R4. Cyber Vulnerability Assessment
R5. Documentation Review and Maintenance

Table B-1. CIP Cyber Security Standards Requirements

System Control Requirement
Standard CIP-006-1 — Physical Security
R1. Physical Security Plan
R2. Physical Access Controls
R3. Monitoring Physical Access
R4. Logging Physical Access
R5. Access Log Retention
R6. Maintenance and Testing
Standard CIP-007-1 — Systems Security Management
R1. Test Procedures
R2. Ports and Services
R3. Security Patch Management
R4. Malicious Software Prevention
R5. Account Management
R6. Security Status Monitoring
R7. Disposal or Redeployment
R8. Cyber Vulnerability Assessment
R9. Documentation Review and Maintenance
Standard CIP-008-1 — Incident Reporting and Response Planning
R1. Cyber Security Incident Response Plan
R2. Cyber Security Incident Documentation
Standard CIP-009-1 — Recovery Plans
R1. Recovery Plans
R2. Exercises
R3. Change Control
R4. Backup and Restore
R5. Testing Backup Media

Table B-2. SP 800-53 Controls

Access Control	
AC-1	Access Control Policy and Procedures
AC-2	Account Management
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-5	Separation of Duties
AC-6	Least Privilege
AC-7	Unsuccessful Login Attempts
AC-8	System Use Notification
AC-9	Previous Logon Notification
AC-10	Concurrent Session Control
AC-11	Session Lock
AC-12	Session Termination
AC-13	Supervision and Review—Access Control
AC-14	Permitted Actions without Identification or Authentication
AC-15	Automated Marking
AC-16	Automated Labeling
AC-17	Remote Access
AC-18	Wireless Access Restrictions
AC-19	Access Control for Portable and Mobile Devices
AC-20	Use of External Information Systems
Awareness and Training	
AT-1	Security Awareness and Training Policy and Procedures
AT-2	Security Awareness
AT-3	Security Training
AT-4	Security Training Records
AT-5	Contacts with Security Groups and Associations

Table B-2. SP 800-53 Controls

Audit and Accountability	
AU-1	Audit and Accountability Policy and Procedures
AU-2	Auditable Events
AU-3	Content of Audit Records
AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failures
AU-6	Audit Monitoring, Analysis, and Reporting
AU-7	Audit Reduction and Report Generation
AU-8	Time Stamps
AU-9	Protection of Audit Information
AU-10	Non-repudiation
AU-11	Audit Record Retention
Certification, Accreditation, and Security Assessments	
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures
CA-2	Security Assessments
CA-3	Information System Connections
CA-4	Security Certification
CA-5	Plan of Action and Milestones
CA-6	Security Accreditation
CA-7	Continuous Monitoring
Configuration Management	
CM-1	Configuration Management Policy and Procedures
CM-2	Baseline Configuration
CM-3	Configuration Change Control
CM-4	Monitoring Configuration Changes
CM-5	Access Restrictions for Change
CM-6	Configuration Settings

Table B-2. SP 800-53 Controls

CM-7	Least Functionality
CM-8	Information System Component Inventory

Contingency Planning	
CP-1	Contingency Planning Policy and Procedures
CP-2	Contingency Plan
CP-3	Contingency Training
CP-4	Contingency Plan Testing and Exercises
CP-5	Contingency Plan Update
CP-6	Alternate Storage Site
CP-7	Alternate Processing Site
CP-8	Telecommunications Services
CP-9	Information System Backup
CP-10	Information System Recovery and Reconstitution
Identification and Authentication	
IA-1	Identification and Authentication Policy and Procedures
IA-2	User Identification and Authentication
IA-3	Device Identification and Authentication
IA-4	Identifier Management
IA-5	Authenticator Management
IA-6	Authenticator Feedback
IA-7	Cryptographic Module Authentication
Incident Response	
IR-1	Incident Response Policy and Procedures
IR-2	Incident Response Training
IR-3	Incident Response Testing and Exercises
IR-4	Incident Handling
IR-5	Incident Monitoring
IR-6	Incident Reporting
IR-7	Incident Response Assistance

Table B-2. SP 800-53 Controls

Maintenance	
MA-1	System Maintenance Policy and Procedures
MA-2	Controlled Maintenance
MA-3	Maintenance Tools
MA-4	Remote Maintenance
MA-5	Maintenance Personnel
MA-6	Timely Maintenance
Media Protection	
MP-1	Media Protection Policy and Procedures
MP-2	Media Access
MP-3	Media Labeling
MP-4	Media Storage
MP-5	Media Transport
MP-6	Media Sanitization and Disposal
Physical and Environmental Protection	
PE-1	Physical and Environmental Protection Policy and Procedures
PE-2	Physical Access Authorizations
PE-3	Physical Access Control
PE-4	Access Control for Transmission Medium
PE-5	Access Control for Display Medium
PE-6	Monitoring Physical Access
PE-7	Visitor Control
PE-8	Access Records
PE-9	Power Equipment and Power Cabling
PE-10	Emergency Shutoff
PE-11	Emergency Power
PE-12	Emergency Lighting
PE-13	Fire Protection
PE-14	Temperature and Humidity Controls
PE-15	Water Damage Protection

Table B-2. SP 800-53 Controls

PE-16	Delivery and Removal
PE-17	Alternate Work Site
PE-18	Location of Information System Components
PE-19	Information Leakage

Planning	
PL-1	Security Planning Policy and Procedures
PL-2	System Security Plan
PL-3	System Security Plan Update
PL-4	Rules of Behavior
PL-5	Privacy Impact Assessment
PL-6	Security-Related Activity Planning
Personnel Security	
PS-1	Personnel Security Policy and Procedures
PS-2	Position Categorization
PS-3	Personnel Screening
PS-4	Personnel Termination
PS-5	Personnel Transfer
PS-6	Access Agreements
PS-7	Third-Party Personnel Security
PS-8	Personnel Sanctions
Risk Assessment	
RA-1	Risk Assessment Policy and Procedures
RA-2	Security Categorization
RA-3	Risk Assessment
RA-4	Risk Assessment Update
RA-5	Vulnerability Scanning
System and Services Acquisition	
SA-1	System and Services Acquisition Policy and Procedures
SA-2	Allocation of Resources
SA-3	Life Cycle Support
SA-4	Acquisitions
SA-5	Information System Documentation
SA-6	Software Usage Restrictions

Table B-2. SP 800-53 Controls

SA-7	User Installed Software
SA-8	Security Engineering Principles
SA-9	External Information System Services
SA-10	Developer Configuration Management
SA-11	Developer Security Testing
System and Communications Protection	
SC-1	System and Communications Protection Policy and Procedures
SC-2	Application Partitioning
SC-3	Security Function Isolation
SC-4	Information Remnance
SC-5	Denial of Service Protection
SC-6	Resource Priority
SC-7	Boundary Protection
SC-8	Transmission Integrity
SC-9	Transmission Confidentiality
SC-10	Network Disconnect
SC-11	Trusted Path
SC-12	Cryptographic Key Establishment and Management
SC-13	Use of Cryptography
SC-14	Public Access Protections
SC-15	Collaborative Computing
SC-16	Transmission of Security Parameters
SC-17	Public Key Infrastructure Certificates
SC-18	Mobile Code
SC-19	Voice Over Internet Protocol
SC-20	Secure Name/Address Resolution Service (Authoritative Source)
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)
SC-22	Architecture and Provisioning for Name/Address Resolution Service
SC-23	Session Authenticity

Table B-2. SP 800-53 Controls

System and Information Integrity	
SI-1	System and Information Integrity Policy and Procedures
SI-2	Flaw Remediation
SI-3	Malicious Code Protection
SI-4	Information System Monitoring Tools and Techniques
SI-5	Security Alerts and Advisories
SI-6	Security Functionality Verification
SI-7	Software and Information Integrity
SI-8	Spam Protection
SI-9	Information Input Restrictions
SI-10	Information Accuracy, Completeness, Validity, and Authenticity
SI-11	Error Handling
SI-12	Information Output Handling and Retention

B.5 Mapping NERC CIPs to Other NIST Publications

This section describes some mappings between the NERC CIPs and NIST publications other than SP 800-53.

As discussed in Section 1.1.2, Correspondence of NERC CIPs to NIST Standards and Guidelines, inspection of the structure and environments of the NERC CIPs and NIST SP 800-53 makes the following generalizations clear:

- Most requirements in the NERC CIPs correspond to countermeasures in SP 800-53. There are exceptions, such as CIP-003, R3, *Exceptions*:
  - **R3.** Exceptions—Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).

- **R3.1.**—Exceptions to the Responsible Entity's cyber security policy must be documented within 30 days of being approved by the senior manager or delegate(s).
- **R3.2.**—Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.
- **R3.3.**—Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

- Measures in the NERC CIPs correspond to assessments, which are primarily addressed in SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems.* Assessment refer to determining the overall effectiveness of the controls, that is, the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Compliance in the NERC CIPs corresponds to certification and accreditation in the NIST SPs, which is addressed in SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*. Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security certification.

These rough generalizations characterize the relationship between the types of content within the respective CIP sections relative to different SPs, without actually commenting on the depth, quality, or rigor pertaining to each.

The NERC CIPs identify "measures [that] will be used to demonstrate compliance with the requirements." The principal federal publication that corresponds to the NERC CIP measures is SP 800-53A, which states: "Once employed within an information system, security controls must be assessed to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system."

B.6 Information Security Policies

A basic premise of the FISMA paradigm is that an organization must have information security policies. It is not possible to differentiate acceptable and unacceptable behavior and conditions without a policy. Enumerating a set of procedures is insufficient.

Threat and business environments are continually changing, and policies must be flexible to anticipate such changes. Organizations must manage information security policies so that they

can evolve with the changing legal, regulatory, and corporate governance requirements. Organizations must enforce their policies consistently and provide proof of conformance and remediation procedures.

MITRE inferred that the NERC drafting group thought that its specifications constituted sufficient policy, and the NERC CIPs were given credit for attempting to constitute policy.

B.7 Criticality and System Definition

There are subtle differences between the ways the NERC CIPs address criticality and the ways FIPS 199 and SP 800-53 address criticality. The NERC CIPs distinguish Cyber Assets as critical and non-critical, levying different sets requirements on each.

FIPS 199 allows the agency to divide its IT components into systems, and then requires the agency to determine the criticality of each system to the agency's mission and potential national-level impacts. That criticality is expressed as LOW, MODERATE, or HIGH. SP 800-53 then prescribes three sets of baseline controls based on the criticality determination assigned during compliance with FIPS 199.

FIPS 199 and SP 800-53 treat all the IT components in one system at the same baseline. NERC, on the other hand, allows agencies to apply its two levels of criticality to IT components individually.

The NERC CIPs define Critical Cyber Assets in terms of essential for reliable operation of facilities, systems, and equipment that if destroyed, damaged, degraded, or otherwise rendered unavailable, would:

- Have a significant impact on the ability of the organization to serve large quantities of customers for an extended period of time
- Have a detrimental impact on the reliability or operability of the Bulk Electric System
- Cause significant risk to public health and safety.

The definition of non-Critical Cyber Assets is implied to be all other Cyber Assets. Various requirements are levied on Critical and non-Critical Cyber Assets.

FIPS 199 establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability): LOW, MODERATE, and HIGH.

The potential impact depends on the consequence, or adverse effect, of the loss of confidentiality, integrity, or availability expected on organizational operations, organizational assets, or individuals. If the adverse effect is limited, the potential impact is LOW. If the adverse effect is serious, the potential impact is MODERATE. If the adverse effect is severe or catastrophic, the potential impact is HIGH.

A control system in the NERC CIPs is oriented around its function. For example, a control system might control an electric power distribution substation. There are IT components in many places through this control system. Some of these IT components are critical; some are non-critical. The substation control system, for example, is a critical system that contains critical and non-critical IT components.

The critical and non-critical IT components are subject to different requirements under the NERC CIPs. This approach of applying different levels of requirements to components of the same system appears to conflict with FIPS 199 and SP 800-53, especially when potential impacts to other organizations and potential national-level impacts are considered in categorizing the information system.

B.8 Mapping Codes

Gradations in the degree of correspondence are captured in code numbers detailed below. These codes are used in Table B-4 to map the NERC CIPs to SP 800-53. Using these codes makes it possible to record more than just the presence of correspondence.

Table B-3. Mapping Codes

Code	Meaning
2	NERC requirements include management responsibilities that are outside the scope of SP 800-53.
3	The NERC requirement has a broader scope than the corresponding SP 800-53 control and may cover multiple 800-53 controls, as well as controls not in 800-53.
7	The subheading of the NERC requirement corresponds to an SP 800-53 countermeasure. This NERC requirements subheading is more encompassing in its scope than the corresponding SP 800-53 countermeasure.
8	The NERC requirement and SP 800-53 countermeasures are essentially equivalent.
9	The NERC requirement is more specific than the SP 800-53 countermeasure.
12	The NERC requirement and the SP 800-53 countermeasure each contain specifics not found in the other.
13	The NERC requirement addresses a subset of the SP 800-53 countermeasure.
14	The NERC standard contains the policy to have a plan. This code gives NERC CIP credit for addressing policy and procedures.
15	NERC requirement contains elements that should be added to SP 800-53
16	The NERC requirement is more limited in scope than the corresponding SP 800-53 countermeasure.
17	The NERC requirement is less specific than the corresponding SP 800-53 countermeasure.
18	The record is part of a business system of records.
22	The requirements in CIP 008 generally correspond to the Incident Response (IR) family in SP 800-53.
23	The requirements in CIP 009 generally correspond to the Contingency Planning (CP) family in SP 800-53.

B.9 Row and Column Counts

Note that Table B-4 contains a count of the number of entries in each row and column. This count shows the number of table entries for each NERC CIP requirement and each SP 800-53 control. This count is a very useful indication of the existence of correspondence between the two documents and the distribution, or spread, of that correspondence.

Addressing the SP 800-53 controls in the rows of the table first, note that a zero count indicates that there is no corresponding NERC CIP requirement. A count of one indicates that there is a unique relationship between the SP 800-53 control and the corresponding NERC CIP requirement. Looking across the row, you can find that correspondence. The numeric code is explained in Section B.7 above. The actual NERC CIP requirement is found by looking at the column heading.

A large number in the row count, greater than or equal to five, indicates that the SP 800-53 control is addressed in a large number of NERC CIP requirements. SP 800-53 has abstracted and collected the requirement as part of a control family, while the NERC CIP has distributed the requirement over multiple standards. Seeing the commonality in the SP 800-53 family could enhance uniformity in responding to the NERC requirements.

Looking at the NERC CIP requirements in the columns of the table, the counts of zero and one have similar utility as the row counts. A large number in the column counts indicates that the NERC CIP requirements include multiple SP 800-53 controls.

High row and column counts are indications of the challenges discussed in Section B.1 of comparing documents.

Table B-4. NERC Cyber Security Standards Requirements

Comparison of NERC Requirements and SP 800-53 Controls			CIP-002				CIP-003						CIP-004				CIP-005					CIP-006						CIP-007									CIP-008		CIP-009					
			R1. Critical Asset Identification Method	R2. Critical Asset Identification	R3. Critical Cyber Asset Identification	R4. Annual Approval	R1. Cyber Security Policy	R2. Leadership	R3. Exceptions	R4. Information Protection	R5. Access Control	R6. Change Control and Confgn Mgmt	R1. Awareness	R2. Training	R3. Personnel Risk Assessment	R4. Access	R1. Electronic Security Perimeter	R2. Electronic Access Controls	R3. Monitoring Electronic Access	R4. Cyber Vulnerability Assessment	R5. Documentation Review and Maintenance	R1. Physical Security Plan	R2. Physical Access Controls	R3. Monitoring Physical Access	R4.Logging Physical Access	R5. Access Log Retention	R6. Maintenance and Testing	R1. Test Procedures	R2. Ports and Services	R3. Security Patch Management	R4. Malicious Software Prevention	R5. Account Management	R6. Security Status Monitoring	R7. Disposal or Redeployment	R8. Cyber Vulnerability Assessment	R9. Documentation Review and Maintenance	R1. Cyber Security Incident Response Plan	R2. Cyber Security Incident Documentation	R1. Recovery Plans	R2. Exercises	R3. Change Control	R4. Backup and Restore	R5. Testing Backup Media
Other – Notes						2	3	2		2	2,7	2					9		18			12								19, 2		21	21					22	23					
SP 800-53 Rev. 1 Controls		Count	2	0	1	1	15	2	2	4	2	1	2	2	2	4	2	11	6	4	16	3	1	1	1	1	2	3	1	1	11	4	3	3	2	4	1	1	2	1	1	2	1
Access Control																																											
AC-1	Access Control P&P	4					3				8					17		13			13	13									13												
AC-2	Account Management	5									13							13			13										13												
AC-3	Access Enforcement	0																																									
AC-4	Information Flow Enforcement	0																																									
AC-5	Separation of Duties	0																																									
AC-6	Least Privilege	1																													13												
AC-7	Unsuccessful Logon Attempts	0																																									
AC-8	System Use Notification	2																8			13																						
AC-9	Previous Logon Notification	0																																									
AC-10	Concurrent Session Control	0																																									
AC-11	Session Lock	0																																									
AC-12	Session Termination	0																																									
AC-13	Supervision and Review—A C	0																																									
AC-14	Permitted Actions without I or A	0																																									
AC-15	Automated Marking	0																																									
AC-16	Automated Labeling	0																																									
AC-17	Remote Access	3															12	9	17		13																							
AC-18	Wireless Access Restrictions	2																17	17																								
AC-19	Access Control for Portable and Mobile Devices	2																17	17																								
AC-20	Use of External Information Systems	0																																									

Table B-4. NERC Cyber Security Standards Requirements

Comparison of NERC Requirements and SP 800-53 Controls			CIP-002				CIP-003						CIP-004				CIP-005					CIP-006						CIP-007									CIP-008		CIP-009					
			R1. Critical Asset Identification Method	R2. Critical Asset Identification	R3. Critical Cyber Asset Identification	R4. Annual Approval	R1. Cyber Security Policy	R2. Leadership	R3. Exceptions	R4. Information Protection	R5. Access Control	R6. Change Control and Confgn Mgmt	R1. Awareness	R2. Training	R3. Personnel Risk Assessment	R4. Access	R1. Electronic Security Perimeter	R2. Electronic Access Controls	R3. Monitoring Electronic Access	R4. Cyber Vulnerability Assessment	R5. Documentation Review and Maintenance	R1. Physical Security Plan	R2. Physical Access Controls	R3. Monitoring Physical Access	R4.Logging Physical Access	R5. Access Log Retention	R6. Maintenance and Testing	R1. Test Procedures	R2. Ports and Services	R3. Security Patch Management	R4. Malicious Software Prevention	R5. Account Management	R6. Security Status Monitoring	R7. Disposal or Redeployment	R8. Cyber Vulnerability Assessment	R9. Documentation Review and Maintenance	R1. Cyber Security Incident Response Plan	R2. Cyber Security Incident Documentation	R1. Recovery Plans	R2. Exercises	R3. Change Control	R4. Backup and Restore	R5. Testing Backup Media
Other – Notes						2	3	2		2	2,7	2					9		18			12								19, 2		21	21					22	23					
SP 800-53 Rev. 1 Controls		Count	2	0	1	1	15	2	2	4	2	1	2	2	2	4	2	11	6	4	16	3	1	1	1	1	2	3	1	1	2	11	4	3	3	2	4	1	2	1	1	2	1
Awareness and Training																																												
AT-1	Security Awareness and Training P&P	2											13	13																														
AT-2	Security Awareness and Literacy Training	1											8																															
AT-3	Specialized Security Training	0																																									
AT-4	Security Training Records	1												8																														
AT-5	Contacts with Security Groups & Associations	0																																										
Audit and Accountability																																												
AU-1	Audit and Accountability P&P	4						3											13		13											13												
AU-2	Auditable Events	3																	13													13	17											
AU-3	Content of Audit Records	1																														17												
AU-4	Audit Storage Capacity	0																																									
AU-5	Response to Audit Processing Failures	0																																									
AU-6	Audit Monitoring, Analysis, and Reporting	3																	13		13											8												
AU-7	Audit Reduction and Report Generation	0																																									
AU-8	Time Stamps	0																																									
AU-9	Protection of Audit Information	0																																									
AU-10	Non-repudiation	0																																									
AU-11	Audit Record Retention	4																	8													8	7					8					

Table B-4. NERC Cyber Security Standards Requirements

Comparison of NERC Requirements and SP 800-53 Controls			CIP-002				CIP-003						CIP-004				CIP-005					CIP-006						CIP-007									CIP-008		CIP-009					
			R1. Critical Asset Identification Method	R2. Critical Asset Identification	R3. Critical Cyber Asset Identification	R4. Annual Approval	R1. Cyber Security Policy	R2. Leadership	R3. Exceptions	R4. Information Protection	R5. Access Control	R6. Change Control and Confgn Mgmt	R1. Awareness	R2. Training	R3. Personnel Risk Assessment	R4. Access	R1. Electronic Security Perimeter	R2. Electronic Access Controls	R3. Monitoring Electronic Access	R4. Cyber Vulnerability Assessment	R5. Documentation Review and Maintenance	R1. Physical Security Plan	R2. Physical Access Controls	R3. Monitoring Physical Access	R4.Logging Physical Access	R5. Access Log Retention	R6. Maintenance and Testing	R1. Test Procedures	R2. Ports and Services	R3. Security Patch Management	R4. Malicious Software Prevention	R5. Account Management	R6. Security Status Monitoring	R7. Disposal or Redeployment	R8. Cyber Vulnerability Assessment	R9. Documentation Review and Maintenance	R1. Cyber Security Incident Response Plan	R2. Cyber Security Incident Documentation	R1. Recovery Plans	R2. Exercises	R3. Change Control	R4. Backup and Restore	R5. Testing Backup Media
Other – Notes						2	3	2		2	2,7	2					9		18			12								19, 2		21	21				22	23						
SP 800-53 Rev. 1 Controls	Count		2	0	1	1	15	2	2	4	2	1	2	2	2	4	2	11	6	4	16	3	1	1	1	1	2	3	1	1	2	11	4	3	3	4	1	2	1	2	1	1	2	1
Certification, Accreditation, and Security Assessments																																												
CA-1	Certification, Accreditation, and Security Assessment P&P	1					3																					13															
CA-2	Security Assessments	5																		13	13						13						8										
CA-3	Information System Connections	2																8			13																							
CA-4	Security Certification	0																																										
CA-5	Plan of Action and Milestones	4								13										8	13												8										
CA-6	Security Accreditation	2						13		8																																		
CA-7	Continuous Monitoring	0																																										
Configuration Management																																												
CM-1	Configuration Management P&P	2					3					7									8																							
CM-2	Baseline Configuration and System Component Inventory	2																			13											13				8	13						
CM-3	Configuration Change Control	3																										15														
CM-4	Monitoring Configuration Changes	1																											13														
CM-5	Access Restrictions for Change	0																																										
CM-6	Configuration Settings	0																																										
CM-7	Least Functionality	3																13			13																							
CM-8	Information System Component Inventory	2			16	16																																						

Table B-4. NERC Cyber Security Standards Requirements

Comparison of NERC Requirements and SP 800-53 Controls			CIP-002				CIP-003						CIP-004				CIP-005					CIP-006						CIP-007									CIP-008		CIP-009					
			R1. Critical Asset Identification Method	R2. Critical Asset Identification	R3. Critical Cyber Asset Identification	R4. Annual Approval	R1. Cyber Security Policy	R2. Leadership	R3. Exceptions	R4. Information Protection	R5. Access Control	R6. Change Control and Confgn Mgmt	R1. Awareness	R2. Training	R3. Personnel Risk Assessment	R4. Access	R1. Electronic Security Perimeter	R2. Electronic Access Controls	R3. Monitoring Electronic Access	R4. Cyber Vulnerability Assessment	R5. Documentation Review and Maintenance	R1. Physical Security Plan	R2. Physical Access Controls	R3. Monitoring Physical Access	R4.Logging Physical Access	R5. Access Log Retention	R6. Maintenance and Testing	R1. Test Procedures	R2. Ports and Services	R3. Security Patch Management	R4. Malicious Software Prevention	R5. Account Management	R6. Security Status Monitoring	R7. Disposal or Redeployment	R8. Cyber Vulnerability Assessment	R9. Documentation Review and Maintenance	R1. Cyber Security Incident Response Plan	R2. Cyber Security Incident Documentation	R1. Recovery Plans	R2. Exercises	R3. Change Control	R4. Backup and Restore	R5. Testing Backup Media
Other – Notes						2	3	2		2	2,7	2					9		18			12								19, 2		21	21					22	23					
SP 800-53 Rev. 1 Controls		Count	2	0	1	1	15	2	2	4	2	1	2	2	2	4	2	11	6	4	16	3	1	1	1	1	2	3	1	1	2	11	4	3	3	2	4	1	2	1	1	1	2	8
Contingency Planning																																												
CP-1	Contingency Planning P&P	2					3																																14				8
CP-2	Contingency Plan	2								3																													8				13
CP-3	Contingency Training	0																																						8				
CP-4	Contingency Plan Testing and Exercises	1																																							8				
CP-5	Contingency Plan Update	1																																										
CP-6	Alternate Storage Site	0																																										
CP-7	Alternate Processing Site	0																																										
CP-8	Telecommunications Services	0																																										
CP-9	IS Backup	2																																										8
CP-10	IS Recovery and Reconstitution	1																																										13
Identification and Authentication																																												
IA-1	Identification and Authentication P&P	2					3																									13												
IA-2	User Identification and Authentication	2																17			13																								
IA-3	Device Identification and Authentication	0																																										
IA-4	Identifier Management	0																																										
IA-5	Authenticator Management	1																														13												
IA-6	Authenticator Feedback	0																																										
IA-7	Cryptographic Module Authentication	0																																										

Table B-4. NERC Cyber Security Standards Requirements

Comparison of NERC Requirements and SP 800-53 Controls		CIP-002				CIP-003						CIP-004				CIP-005					CIP-006						CIP-007									CIP-008		CIP-009					
		R1. Critical Asset Identification Method	R2. Critical Asset Identification	R3. Critical Cyber Asset Identification	R4. Annual Approval	R1. Cyber Security Policy	R2. Leadership	R3. Exceptions	R4. Information Protection	R5. Access Control	R6. Change Control and Confgn Mgmt	R1. Awareness	R2. Training	R3. Personnel Risk Assessment	R4. Access	R1. Electronic Security Perimeter	R2. Electronic Access Controls	R3. Monitoring Electronic Access	R4. Cyber Vulnerability Assessment	R5. Documentation Review and Maintenance	R1. Physical Security Plan	R2. Physical Access Controls	R3. Monitoring Physical Access	R4.Logging Physical Access	R5. Access Log Retention	R6. Maintenance and Testing	R1. Test Procedures	R2. Ports and Services	R3. Security Patch Management	R4. Malicious Software Prevention	R5. Account Management	R6. Security Status Monitoring	R7. Disposal or Redeployment	R8. Cyber Vulnerability Assessment	R9. Documentation Review and Maintenance	R1. Cyber Security Incident Response Plan	R2. Cyber Security Incident Documentation	R1. Recovery Plans	R2. Exercises	R3. Change Control	R4. Backup and Restore	R5. Testing Backup Media
Other – Notes					2	3	2		2	2,7	2					9		18			12								19, 2		21	21				22	23					
SP 800-53 Rev. 1 Controls	Count	2	0	1	1	15	2	2	4	2	1	2	2	2	4	2	11	6	4	16	3	1	1	1	1	2	3	1	1	2	11	4	3	3	2	4	1	2	1	1	2	1
Incident Response																																										
IR-1	Incident Response P&P	2				3																															8					
IR-2	Incident Response Training	0																																								
IR-3	Incident Response Testing and Exercises	1																																			9					
IR-4	Incident Handling	1																																			9					
IR-5	Incident Monitoring	0																																								
IR-6	Incident Reporting	1																																			9					
IR-7	Incident Response Assistance	0																																								
Maintenance																																										
MA-1	System Maintenance P&P	2				3																				13																	
MA-2	Controlled Maintenance	0																																								
MA-3	Maintenance Tools	0																																								
MA-4	Remote Maintenance	0																																								
MA-5	Maintenance Personnel	0																																								
MA-6	Timely Maintenance	0																																								
Media Protection																																										
MP-1	Media Protection P&P	2				3																												14								
MP-2	Media Access	0																																								
MP-3	Media Labeling	0																																								
MP-	Media Storage	0																																								
MP-5	Media Transport	0																																								
MP-6	Media Sanitization and Disposal	1																																8								

Table B-4. NERC Cyber Security Standards Requirements

Comparison of NERC Requirements and SP 800-53 Controls			CIP-002				CIP-003						CIP-004				CIP-005					CIP-006						CIP-007									CIP-008		CIP-009				
			R1. Critical Asset Identification Method	R2. Critical Asset Identification	R3. Critical Cyber Asset Identification	R4. Annual Approval	R1. Cyber Security Policy	R2. Leadership	R3. Exceptions	R4. Information Protection	R5. Access Control	R6. Change Control and Confgn Mgmt	R1. Awareness	R2. Training	R3. Personnel Risk Assessment	R4. Access	R1. Electronic Security Perimeter	R2. Electronic Access Controls	R3. Monitoring Electronic Access	R4. Cyber Vulnerability Assessment	R5. Documentation Review and Maintenance	R1. Physical Security Plan	R2. Physical Access Controls	R3. Monitoring Physical Access	R4.Logging Physical Access	R5. Access Log Retention	R6. Maintenance and Testing	R1. Test Procedures	R2. Ports and Services	R3. Security Patch Management	R4. Malicious Software Prevention	R5. Account Management	R6. Security Status Monitoring	R7. Disposal or Redeployment	R8. Cyber Vulnerability Assessment	R9. Documentation Review and Maintenance	R1. Cyber Security Incident Response Plan	R2. Cyber Security Incident Documentation	R1. Recovery Plans	R2. Exercises	R3. Change Control	R4. Backup and Restore	R5. Testing Backup Media
Other – Notes						2	3	2		2	2,7	2					9		18			12								19, 2		21	21				22	23					
SP 800-53 Rev. 1 Controls	Count		2	0	1	1	15	2	2	4	2	1	2	2	2	4	2	11	6	4	16	3	1	1	1	1	2	3	1	1	2	11	4	3	3	2	4	1	2	1	1	2
Physical and Environmental Protection																																										
PE-1	Physical and Environmental Protection P&P	2					3															12																					
PE-2	Physical Access Authorizations	0																																								
PE-3	Physical Access Control	2																					8	8																			
PE-4	Access Control for Transmission Medium	0																																								
PE-5	Access Control for Display Medium	0																																								
PE-6	Monitoring Physical Access	1																							9																		
PE-7	Visitor Control	1																				7				13																	
PE-8	Access Records	1																																								
PE-9	Power Equipment and Power Cabling	0																																								
PE-10	Emergency Shutoff	0																																								
PE-11	Emergency Power	0																																								
PE-12	Emergency Lighting	0																																								
PE-13	Fire Protection	0																																								
PE-14	Temperature and Humidity Controls	0																																								
PE-15	Water Damage Protection	0																																								
PE-16	Delivery and Removal	0																																								
PE-17	Alternate Work Site	0																																								
PE-18	Location of Information System Components	0																																								
PE-19	Information Leakage	0																																								

Table B-4. NERC Cyber Security Standards Requirements

Comparison of NERC Requirements and SP 800-53 Controls			CIP-002				CIP-003						CIP-004				CIP-005					CIP-006						CIP-007									CIP-008		CIP-009					
			R1. Critical Asset Identification Method	R2. Critical Asset Identification	R3. Critical Cyber Asset Identification	R4. Annual Approval	R1. Cyber Security Policy	R2. Leadership	R3. Exceptions	R4. Information Protection	R5. Access Control	R6. Change Control and Confign Mgmt	R1. Awareness	R2. Training	R3. Personnel Risk Assessment	R4. Access	R1. Electronic Security Perimeter	R2. Electronic Access Controls	R3. Monitoring Electronic Access	R4. Cyber Vulnerability Assessment	R5. Documentation Review and Maintenance	R1. Physical Security Plan	R2. Physical Access Controls	R3. Monitoring Physical Access	R4.Logging Physical Access	R5. Access Log Retention	R6. Maintenance and Testing	R1. Test Procedures	R2. Ports and Services	R3. Security Patch Management	R4. Malicious Software Prevention	R5. Account Management	R6. Security Status Monitoring	R7. Disposal or Redeployment	R8. Cyber Vulnerability Assessment	R9. Documentation Review and Maintenance	R1. Cyber Security Incident Response Plan	R2. Cyber Security Incident Documentation	R1. Recovery Plans	R2. Exercises	R3. Change Control	R4. Backup and Restore	R5. Testing Backup Media
Other – Notes						2	3	2		2	2,7	2					9		18			12								19, 2		21	21					22	23					
SP 800-53 Rev. 1 Controls		Count	2	0	1	1	15	2	2	4	2	1	2	2	2	4	2	11	6	4	16	3	1	1	1	1	2	3	1	1	2	11	4	3	3	2	4	1	2	1	1	2	1
Planning																																												
PL-1	Security Planning P&P	1					3																					7															
PL-2	System Security Plan	1							13																																		
PL-3	System Security Plan Update	1							13																																		
PL-4	Rules of Behavior	0																																									
PL-5	Privacy Impact Assessment	0																																									
PL-6	Security-Related Activity Planning	1																																									
Personnel Security																																											
PS-1	Personnel Security P&P	2					3								13																												
PS-2	Position Categorization	0																																									
PS-3	Risk Assessment Personnel Termination	1													13																													
PS-4	Personnel Termination	2														13																13											
PS-5	Personnel Transfer	2														8																13											
PS-6	Access Agreements	0																																									
PS-7	Third-Party Personnel Security	1														13																												
PS-8	Personnel Sanctions	0																																									
Risk Assessment																																											
RA-1	Risk Assessment P&P	4	14				3													13	13																						
RA-2	Security Categorization	1								17																																	
RA-3	Risk Assessment	1	16																													75											
RA-4	Risk Assessment Update	0																																									
RA-5	Vulnerability Scanning	4																		13	13													13										

Table B-4. NERC Cyber Security Standards Requirements

Comparison of NERC Requirements and SP 800-53 Controls			CIP-002				CIP-003						CIP-004				CIP-005					CIP-006						CIP-007									CIP-008		CIP-009					
			R1. Critical Asset Identification Method	R2. Critical Asset Identification	R3. Critical Cyber Asset Identification	R4. Annual Approval	R1. Cyber Security Policy	R2. Leadership	R3. Exceptions	R4. Information Protection	R5. Access Control	R6. Change Control and Confgn Mgmt	R1. Awareness	R2. Training	R3. Personnel Risk Assessment	R4. Access	R1. Electronic Security Perimeter	R2. Electronic Access Controls	R3. Monitoring Electronic Access	R4. Cyber Vulnerability Assessment	R5. Documentation Review and Maintenance	R1. Physical Security Plan	R2. Physical Access Controls	R3. Monitoring Physical Access	R4.Logging Physical Access	R5. Access Log Retention	R6. Maintenance and Testing	R1. Test Procedures	R2. Ports and Services	R3. Security Patch Management	R4. Malicious Software Prevention	R5. Account Management	R6. Security Status Monitoring	R7. Disposal or Redeployment	R8. Cyber Vulnerability Assessment	R9. Documentation Review and Maintenance	R1. Cyber Security Incident Response Plan	R2. Cyber Security Incident Documentation	R1. Recovery Plans	R2. Exercises	R3. Change Control	R4. Backup and Restore	R5. Testing Backup Media
Other – Notes						2	3	2		2	2,7	2					9		18			12								19, 2		21	21					22	23					
SP 800-53 Rev. 1 Controls		Count	2	0	1	1	15	2	2	4	2	1	2	2	2	4	2	11	6	4	16	3	1	1	1	1	2	3	1	1	2	11	4	3	3	2	4	1	2	1	1	2	1
System and Services Acquisition																																												
SA-1	System and Services Acquisition P&P	1					3																																				
SA-2	Allocation of Resources	0																																									
SA-3	Life Cycle Support	0																																									
SA-4	Acquisitions	0																																									
SA-5	Information System Documentation	0																																									
SA-6	Software Usage Restrictions	0																																									
SA-7	User Installed Software	0																																									
SA-8	Security Engineering Principles	0																																									
SA-9	External Information System Services	0																																									
SA-10	Developer Configuration Management	0																																									
SA-11	Developer Security Testing	0																																									
System and Communications Protection																																												
SC-1	System and Communications Protection P&P	3					3											13			13																							
SC-2	Application Partitioning	0																																									
SC-3	Security Function Isolation	0																																									
SC-4	Information Remnants	0																																									
SC-5	Denial of Service Protection	0																																									
SC-6	Resource Priority	0																																									
SC-7	Boundary Protection	3															12	12			13																							
SC-8	Transmission Integrity	0																																									

Table B-4. NERC Cyber Security Standards Requirements

Comparison of NERC Requirements and SP 800-53 Controls			CIP-002				CIP-003						CIP-004				CIP-005					CIP-006						CIP-007									CIP-008		CIP-009					
			R1. Critical Asset Identification Method	R2. Critical Asset Identification	R3. Critical Cyber Asset Identification	R4. Annual Approval	R1. Cyber Security Policy	R2. Leadership	R3. Exceptions	R4. Information Protection	R5. Access Control	R6. Change Control and Confign Mgmt	R1. Awareness	R2. Training	R3. Personnel Risk Assessment	R4. Access	R1. Electronic Security Perimeter	R2. Electronic Access Controls	R3. Monitoring Electronic Access	R4. Cyber Vulnerability Assessment	R5. Documentation Review and Maintenance	R1. Physical Security Plan	R2. Physical Access Controls	R3. Monitoring Physical Access	R4.Logging Physical Access	R5. Access Log Retention	R6. Maintenance and Testing	R1. Test Procedures	R2. Ports and Services	R3. Security Patch Management	R4. Malicious Software Prevention	R5. Account Management	R6. Security Status Monitoring	R7. Disposal or Redeployment	R8. Cyber Vulnerability Assessment	R9. Documentation Review and Maintenance	R1. Cyber Security Incident Response Plan	R2. Cyber Security Incident Documentation	R1. Recovery Plans	R2. Exercises	R3. Change Control	R4. Backup and Restore	R5. Testing Backup Media
Other – Notes						2	3	2		2	2,7	2				4	9		18			12								19, 2		21	21					22	23					
SP 800-53 Rev. 1 Controls		Count	2	0	1	1	15	2	2	4	2	1	2	2	2	4	2	11	6	4	16	3	1	1	1	1	2	3	1	1	11	4	3	3	2	4	1	1	2	1	1	2	1
SC-9	Transmission Confidentiality	0																																									
SC-10	Network Disconnect	0																																									
SC-11	Trusted Path	0																																								
SC-12	Cryptographic Key Establishment and Management	0																																								
SC-13	Use of Validated Cryptography	0																																								
SC-14	Public Access Protections	0																																								
SC-15	Collaborative Computing	0																																								
SC-16	Transmission of Security Parameters	0																																								
SC-17	Public Key Infrastructure Certificates	0																																								
SC-18	Mobile Code	0																																								
SC-19	Voice Over Internet Protocol	0																																								
SC-20	Secure Name Lookup Service (Authoritative Source)	0																																								
SC-21	Secure Name Lookup Service (Resolution)	0																																								
SC-22	Architecture and Provisioning for Name/Address Resolution Service	0																																								
SC-23	Session Authenticity	0																																								

Table B-4. NERC Cyber Security Standards Requirements

Comparison of NERC Requirements and SP 800-53 Controls			CIP-002				CIP-003						CIP-004				CIP-005					CIP-006						CIP-007									CIP-008		CIP-009					
			R1. Critical Asset Identification Method	R2. Critical Asset Identification	R3. Critical Cyber Asset Identification	R4. Annual Approval	R1. Cyber Security Policy	R2. Leadership	R3. Exceptions	R4. Information Protection	R5. Access Control	R6. Change Control and Confgn Mgmt	R1. Awareness	R2. Training	R3. Personnel Risk Assessment	R4. Access	R1. Electronic Security Perimeter	R2. Electronic Access Controls	R3. Monitoring Electronic Access	R4. Cyber Vulnerability Assessment	R5. Documentation Review and Maintenance	R1. Physical Security Plan	R2. Physical Access Controls	R3. Monitoring Physical Access	R4.Logging Physical Access	R5. Access Log Retention	R6. Maintenance and Testing	R1. Test Procedures	R2. Ports and Services	R3. Security Patch Management	R4. Malicious Software Prevention	R5. Account Management	R6. Security Status Monitoring	R7. Disposal or Redeployment	R8. Cyber Vulnerability Assessment	R9. Documentation Review and Maintenance	R1. Cyber Security Incident Response Plan	R2. Cyber Security Incident Documentation	R1. Recovery Plans	R2. Exercises	R3. Change Control	R4. Backup and Restore	R5. Testing Backup Media
Other – Notes						2	3	2		2	2,7	2					9		18			12								19, 2		21	21					22	23					
SP 800-53 Rev. 1 Controls		Count	2	0	1	1	15	2	2	4	2	1	2	2	2	4	2	11	6	4	16	3	1	1	1	1	2	3	1	1	2	11	4	3	3	2	4	1	2	1	1	2	2
System and Information Integrity																																												
SI-1	System and Information Integrity P&P	1					3																																				
SI-2	Flaw Remediation	1																											13														
SI-3	Malicious Code Protection	1																												8													
SI-4	Information System Monitoring Tools and Techniques	2																												13		8											
SI-5	Security Alerts and Advisories	0																																									
SI-6	Security Functionality Verification	0																																									
SI-7	Software and Information Integrity	0																																									
SI-8	Spam Protection	0																																									
SI-9	Information Input Restrictions	0																																									
SI-10	Information Accuracy, Completeness, Validity and Authenticity	0																																									
SI-11	Error Handling	0																																									
SI-12	Information Output Handling and Retention	0																																									

Appendix C Detailed Requirements Comparison between the NERC CIPs and SP 800-53

This appendix presents a detailed comparison of the SP 800-53 requirements to the NERC CIPs. As summarized in Table B-4, the SP 800-53 controls are a superset of the NERC CIP requirements. The Moderate Baseline control set in SP 800-53 covers the NERC CIP requirements.

C.1 Documentation Requirements

Both SP 800-53 and the NERC CIPs contain explicit requirements for the production of documents that establish policy and procedures. There are also requirements for maintaining records of actions performed (i.e., recording that an action has taken place and its result).

Documents must be written in human readable natural language, and may be contained on or in any media, including digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm).

C.2 Assurance Requirements

SP 800-53 distinguishes between functional security controls that encompass manual and automated policies and practices and are selected to reduce potential impact to an acceptable level–summarized in its Appendix D and detailed in its Appendix F–and assurance requirements in Appendix E that specify the activities and actions that establish confidence in the controls. In the NERC CIPs, functional and assurance requirements are intertwined.

The SP 800-53 assurance requirements, described in its Appendix E, are directed at the activities and actions that security control developers and implementers[10] define and apply to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The assurance requirements are applied on a control-by-control basis. The requirements are grouped by security control baseline (i.e., LOW, MODERATE, and HIGH) because the requirements apply to each control within the respective baseline. Assurance requirements address whether:

- The security control is in effect and meets explicitly identified functional requirements in the control statement.

[10] In this context, a developer/implementer is an individual or group of individuals responsible for the development or implementation of security controls for an information system. This may include, for example, hardware and software vendors providing the controls; contractors implementing the controls; or organizational personnel such as information system owners, information system security officers, system and network administrators, or other individuals with security responsibility for the information system.

- The control developer/implementer provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control.
- The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will meet its required function or purpose.

These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

C.3 Detailed Requirements Comparison

As seen in Table C-1, most requirements in the NERC CIPs correspond to SP 800-53 controls. As discussed in Section 2.3.2, the procedure for applying the NERC CIPs is to first identify Critical Assets that support the reliable operation of the Bulk Electric System. The second step is to identify the Critical Cyber Assets that are essential to the Critical Assets. Requirements in the NERC CIPs that deal with corporate governance are identified in Table C-2.

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Access Control			
AC-1 Access Control Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-003 R1.1	[The Responsible Entity shall…ensure…] The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
		CIP-003 R1.3	[The Responsible Entity shall…ensure…] Annual review and approval of the cyber security policy by the senior manager assigned pursuant to [CIP-003] R2.
		CIP-003 R5 Access Control	The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
		CIP-003 R5.3	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.
		CIP-005 R2.1	These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
AC-2 Account Management	The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment: organization-defined frequency, at least annually*]. The organization employs automated mechanisms to support the management of information system accounts.	CIP-003 R5.1	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information. • Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access. • The list of personnel responsible for authorizing access to protected information shall be verified at least annually.
	The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].	CIP-003 R5.2	The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
	The information system automatically disables inactive accounts after [Assignment: organization-defined time period].	CIP-004 R4 Access R4.1	The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly….
	The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.	CIP-005 R2.5	The required documentation shall, at least, identify and describe the review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.
		CIP-005 R5 Documentation Review and Maintenance r5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
		CIP-007 R5.1.3	The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.
		CIP-007 R5.2	The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts. • The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service. The Responsible Entity shall identify those individuals with access to shared accounts.
AC-3 Access Enforcement	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy. The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
AC-4 Information Flow Enforcement	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.		
AC-5 Separation of Duties	The information system enforces separation of duties through assigned access authorizations.		
AC-6 Least Privilege	The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.	CIP-007 R5.1	The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
AC-7 Unsuccessful Logon Attempts	The information system enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*] time period. The information system automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*], *delays next login prompt according to Assignment: organization-defined delay algorithm.*]] when the maximum number of unsuccessful attempts is exceeded.		
AC-8 System Use Notification	The information system displays an approved system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.	CIP-005 R2.6 Appropriate Use Banner	Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
AC-9 Previous Logon Notification	Control Not Selected in the Moderate Baseline		
AC-10 Concurrent Session Control	Control Not Selected in the Moderate Baseline		
AC-11 Session Lock	The information system prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures..		
AC-12 Session Termination	The information system automatically terminates a remote session after [*Assignment: organization-defined time period*] of inactivity.		
AC-13 Supervision and Review—Access Control	The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls. The organization employs automated mechanisms to facilitate the review of user activities.		
AC-14 Permitted Actions without Identification or Authentication	The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication. The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
AC-15 Automated Marking	Control Not Selected in Moderate Baseline		
AC-16 Automated Labeling	Control Not Selected in Moderate Baseline		
AC-17 Remote Access	The organization authorizes, monitors, and controls all methods of remote access to the information system. The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. The organization controls all remote accesses through a limited number of managed access control points. The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	CIP-005 R1.1	Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
		CIP-005 R2.3	The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).
		CIP-005 R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
		CIP-005 R2.5	The required documentation shall, at least, identify and describe the controls used to secure dial-up accessible connections.
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
AC-18 Wireless Access Restrictions	The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, and controls wireless access to the information system. The organization uses authentication and encryption to protect wireless access to the information system.	CIP-005 R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
AC-19 Access Control for Portable and Mobile Devices	The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.	CIP-005 R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
AC-20 Use of External Information Systems	The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Awareness and Training			
AT-1 Security Awareness and Training Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	CIP-004 R1 Awareness	The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices.
		CIP-004 R2 Training	The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary. • This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization. • Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities: – The proper use of Critical Cyber Assets; – Physical and electronic access controls to Critical Cyber Assets; – The proper handling of Critical Cyber Asset information; and, – Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.
AT-2 Security Awareness and Literacy Training	The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [*Assignment: organization-defined frequency, at least annually*] thereafter.	CIP-003 R1.2	[The Responsible Entity shall…ensure…] The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.
AT-3 Specialized Security Training	The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.		
AT-4 Security Training Records	The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.	CIP-004 R2.3	The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.
AT-5 Contacts with Security Groups & Associations	Control Not Selected in Moderate Baseline		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Audit and Accountability			
AU-1 Audit and Accountability Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-003 R1.1	[The Responsible Entity shall…ensure…] The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
		CIP-003 R1.3	[The Responsible Entity shall…ensure…] Annual review and approval of the cyber security policy by the senior manager assigned pursuant to [CIP-003] R2.
		CIP-005 R3 Monitoring Electronic Access	The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
		CIP-007 R5 Account Management	The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
		CIP-007 R5.2.3	Where accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
AU-2 Auditable Events	The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*]. The organization periodically reviews and updates the list of organization-defined auditable events.	CIP-005 R3.1	For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
		CIP-007 R5.1.2	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.
		CIP-007 R5.2.3	Where accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
		CIP-007 R6.1	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
		CIP-007 R6.3	The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
AU-3 Content of Audit Records	The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.	CIP-007 R5.1.2	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.
		CIP-007 R5.2.3	Where accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
AU-4 Audit Storage Capacity	The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.		
AU-5 Response to Audit Processing Failures	The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
AU-6 Audit Monitoring, Analysis, and Reporting	The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].	CIP-005 R3.2	Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
		CIP-007 R6.5	The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.
		CIP-007 R6.2	The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
AU-7 Audit Reduction and Report Generation	The information system provides an audit reduction and report generation capability. The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.		
AU-8 Time Stamps	The information system provides time stamps for use in audit record generation. The organization synchronizes internal information system clocks [*Assignment: organization-defined frequency*].		
AU-9 Protection of Audit Information	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.		
AU-10 Non-repudiation	Control Not Selected in Moderate Baseline		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
AU-11 Audit Record Retention	The organization retains audit records for [*Assignment: organization-defined time period*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	CIP-005 R5.3	The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.
		CIP-007 R5.1.2	The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.
		CIP-007 R6.4	The Responsible Entity shall retain all logs specified in CIP-007 Requirement R6 for ninety calendar days.
		CIP-008 R2 Cyber Security Incident Documentation	The Responsible Entity shall keep relevant documentation related to Cyber Security Incidents reportable per Requirement R1.1 for three calendar years.

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Certification, Accreditation, and Security Assessments			
CA-1 Certification, Accreditation, and Security Assessment Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.	CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-003 R1.1	[The Responsible Entity shall…ensure…] The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
		CIP-003 R1.3	[The Responsible Entity shall…ensure…] Annual review and approval of the cyber security policy by the senior manager assigned pursuant to [CIP-003] R2.

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
CA-2 Security Assessments	The organization conducts an assessment of the security controls in the information system [*Assignment: organization-defined frequency, at least annually*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	CIP-005 R4 Cyber Vulnerability Assessment	The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually….
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
		CIP-006 R6 Maintenance and Testing	The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following: • Testing and maintenance of all physical security mechanisms on a cycle no longer than three years. • Retention of testing and maintenance records for the cycle determined. • Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.
		CIP-007 R1 Test Procedures	The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware…. • The Responsible Entity shall document that testing is performed in a manner that reflects the production environment. • The Responsible Entity shall document test results.
		CIP-007 R8 Cyber Vulnerability Assessment	The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following: • A document identifying the vulnerability assessment process; • A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled; • A review of controls for default accounts; and, • Documentation of the results of the assessment

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
CA-3 Information System Connections	The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.	CIP-005 R2 Electronic Access Controls	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s). [See also SC1 and SC-7]
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
CA-4 Security Certification	The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.		
CA-5 Plan of Action and Milestones	The organization develops and updates [*Assignment: organization-defined frequency*], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.	CIP-003 R4.3	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.
		CIP-005 R4.5	The vulnerability assessment shall include, at a minimum,… documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
		CIP-007 R8.4	[The vulnerability assessment shall include…] Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.
CA-6 Security Accreditation	The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [*Assignment: organization-defined frequency, at least every three years*] or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.	CIP-003 R2.3	The senior manager or delegate(s) [identified per CIP-003 R2], shall authorize and document any exception from the requirements of the cyber security policy.
		CIP-003 R4.3	The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results….
CA-7 Continuous Monitoring	The organization monitors the security controls in the information system on an ongoing basis.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Configuration Management			
CM-1 Configuration Management Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	CIP-003 R6 Change Control and Configuration Management	The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.
		CIP-003 R1.3	[The Responsible Entity shall…ensure…] Annual review and approval of the cyber security policy by the senior manager assigned pursuant to [CIP-003] R2.
CM-2 Baseline Configuration and System Component Inventory	The organization develops, documents, and maintains a current baseline configuration of the information system. The organization updates the baseline configuration of the information system as an integral part of information system component installations.	CIP-007 R9 Documentation Review and Maintenance	The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.
CM-3 Configuration Change Control	The organization authorizes, documents, and controls changes to the information system.	CIP-005 R5.2	The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change
		CIP-007 R3 Security Patch Management	The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
		CIP-007 R9 Documentation Review and Maintenance	The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.
CM-4 Monitoring Configuration Changes	The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.	CIP-007 R1 Test Procedures	The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls.
CM-5 Access Restrictions for Change	The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes.		
CM-6 Configuration Settings	The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
CM-7 Least Functionality	The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services*].	CIP-005 R2.2	At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
		CIP-007 R2 Ports and Services	The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled. The Responsible Entity shall enable only those ports and services required for normal and emergency operations. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s). In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.
CM-8 Information System Component Inventory	The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information. The organization updates the inventory of information system components as an integral part of component installations.	CIP-002 R3 Critical Cyber Asset Identification	…The Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset.... The Responsible Entity shall review this list at least annually, and update it as necessary….
		CIP-002 R4 Annual Approval	A senior manager or delegate(s) shall approve annually the list ... of Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the list of ... of Critical Cyber Assets (even if such lists are null.)

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Contingency Planning			
CP-1 Contingency Planning Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	CIP-003 R1.3	[The Responsible Entity shall…ensure…] Annual review and approval of the cyber security policy by the senior manager assigned pursuant to [CIP-003] R2.
		CIP-009 R1 Recovery Plans	The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets.
CP-2 Contingency Plan	The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel. The organization coordinates contingency plan development with organizational elements responsible for related plans.	CIP-009 R1.1 R1.2	The recovery plan(s) shall address at a minimum the following: • Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s). • Define the roles and responsibilities of responders.
CP-3 Contingency Training	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].		
CP-4 Contingency Plan Testing and Exercises	The organization: (i) tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions. The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.	CIP-009 R2 Exercises	The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.
CP-5 Contingency Plan Update	The organization reviews the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	CIP-009 R3 Change Control	Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change.
CP-6 Alternate Storage Site	The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information. The organization identifies an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards. The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
CP-7 Alternate Processing Site	The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [*Assignment: organization-defined time period*] when the primary processing capabilities are unavailable. The organization identifies an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards. The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.		
CP-8 Telecommunications Services	The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable. The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements. The organization obtains alternate telecommunications services that do not share a single point of failure with primary telecommunications services.		
CP-9 Information System Backup	The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [*Assignment: organization-defined frequency*] and protects backup information at the storage location. The organization tests backup information [*Assignment: organization-defined frequency]* to verify media reliability and information integrity. The organization protects system backup information from unauthorized modification.	CIP-009 R4 Backup and Restore	The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.
		CIP-009 R5 Testing Backup Media	Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.
CP-10 Information System Recovery and Reconstitution	The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.	CIP-009 R4 Backup and Restore	The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc.

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Identification and Authentication			
IA-1 Identification and Authentication Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-003 R1.1	[The Responsible Entity shall…ensure…] The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
		CIP-003 R1.3	[The Responsible Entity shall…ensure…] Annual review and approval of the cyber security policy by the senior manager assigned pursuant to [CIP-003] R2.
		CIP-007 R5 Account Management	The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
IA-2 User Identification and Authentication	The information system uniquely identifies and authenticates users (or processes acting on behalf of users). The information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 [*Selection: organization-defined level 3, level 3 using a hardware authentication device, or level 4*] compliant.	CIP-005 R2.4	Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
		CIP-005 R2.5	The required documentation shall, at least, identify and describe: • The processes for access request and authorization. • The authentication methods.
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
IA-3 Device Identification and Authentication	The information system identifies and authenticates specific devices before establishing a connection.		
IA-4 Identifier Management	The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [*Assignment: organization-defined time period*] of inactivity; and (vi) archiving user identifiers.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
IA-5 Authenticator Management	The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	CIP-007 R5.2.1	[For administrator, shared, and other generic accounts] the policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.
		CIP-007 R5.3	At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible: • Each password shall be a minimum of six characters. • Each password shall consist of a combination of alpha, numeric, and "special" characters. Each password shall be changed at least annually, or more frequently based on risk.
IA-6 Authenticator Feedback	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.		
IA-7 Cryptographic Module Authentication	The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Incident Response			
IR-1 Incident Response Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-008R1 Cyber Security Incident Response Plan	The Responsible Entity shall develop and maintain a Cyber Security Incident response plan.… *Note, CIP-008 never explicitly directs implementation of this plan. That intent is inferred from the documentation and testing requirements.*
		CIP-008 R1.2	[The Cyber Security Incident Response plan shall address…] Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.
		CIP-008 R1.4	[The Cyber Security Incident Response plan shall address…] Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.
		CIP-008 R1.5	[The Cyber Security Incident Response plan shall address…] Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.
IR-2 Incident Response Training	The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].		
IR-3 Incident Response Testing and Exercises	The organization tests and/or exercises the incident response capability for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results	CIP-008 R1.6	[The Cyber Security Incident Response plan shall address…] Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.
IR-4 Incident Handling	The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. The organization employs automated mechanisms to support the incident handling process.	CIP-008 R1.1	[The Cyber Security Incident Response plan shall address…] Procedures to characterize and classify events as reportable Cyber Security Incidents.
IR-5 Incident Monitoring	The organization tracks and documents information system security incidents on an ongoing basis.		
IR-6 Incident Reporting	The organization promptly reports incident information to appropriate authorities. The organization employs automated mechanisms to assist in the reporting of security incidents.	CIP-008 R1.3	[The Cyber Security Incident Response plan shall address…] Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
IR-7 Incident Response Assistance	The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability. The organization employs automated mechanisms to increase the availability of incident response-related information and support.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Maintenance			
MA-1 System Maintenance Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-003 R1.1	[The Responsible Entity shall…ensure…] The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
		CIP-003 R1.3	[The Responsible Entity shall…ensure…] Annual review and approval of the cyber security policy by the senior manager assigned pursuant to [CIP-003] R2.
		CIP-006 R6 Maintenance and Testing	The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following: • Testing and maintenance of all physical security mechanisms on a cycle no longer than three years. • Retention of testing and maintenance records for the cycle determined. • Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.
MA-2 Controlled Maintenance	The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements. The organization maintains maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).		
MA-3 Maintenance Tools	The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.		
MA-4 Remote Maintenance	The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed. The organization audits all remote maintenance and diagnostic sessions and appropriate organizational personnel review the maintenance records of the remote sessions. The organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.		
MA-5 Maintenance Personnel	The organization allows only authorized personnel to perform maintenance on the information system.		
MA-6 Timely Maintenance	The organization obtains maintenance support and spare parts for [*Assignment: organization-defined list of key information system components*] within [*Assignment: organization-defined time period*] of failure.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Media Protection			
MP-1 Media Protection Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-003 R1.1	[The Responsible Entity shall…ensure…] The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
		CIP-003 R1.3	[The Responsible Entity shall…ensure…] Annual review and approval of the cyber security policy by the senior manager assigned pursuant to [CIP-003] R2.
		CIP-007 R7 Disposal or Redeployment	The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
MP-2 Media Access	The organization restricts access to information system media to authorized individuals. The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.		
MP-3 Media Labeling	Control Not Selected in Moderate Baseline		
MP-4 Media Storage	The organization physically controls and securely stores information system media within controlled areas.		
MP-5 Media Transport	The organization protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel. The organization protects digital and non-digital media during transport outside of controlled areas using [*Assignment: organization-defined security measures, e.g., locked container, cryptography*]. The organization documents, where appropriate, activities associated with the transport of information system media using [*Assignment: organization-defined system of records*].		
MP-6 Media Sanitization and Disposal	The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse.	CIP-007 R7.1 R7.2 R7.3	Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Physical and Environmental Protection			
PE-1 Physical and Environmental Protection Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-003 R1.1	[The Responsible Entity shall…ensure…] The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
		CIP-003 R1.3	[The Responsible Entity shall…ensure…] Annual review and approval of the cyber security policy by the senior manager assigned pursuant to [CIP-003] R2.
		CIP-003 R5.3	The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.
		CIP-006 R1 Physical Security Plan	The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following: • Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets. • Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points. • Processes, tools, and procedures to monitor physical access to the perimeter(s). • Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls. • Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4. • Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access. • Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls. Process for ensuring that the physical security plan is reviewed at least annually.

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
PE-2 Physical Access Authorizations	The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [*Assignment: organization-defined frequency, at least annually*].		
PE-3 Physical Access Control	The organization controls all physical access points (including designated entry/ exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.	CIP-006 R2 Physical Access Controls	The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods: • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another. • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems. • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station. • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.
		CIP-006 R3 Monitoring Physical Access	The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used: • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response. • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in [CIP-006] Requirement R2.3.
PE-4 Access Control for Transmission Medium	Control Not Selected in Moderate Baseline		
PE-5 Access Control for Display Medium	The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
PE-6 Monitoring Physical Access	The organization monitors physical access to the information system to detect and respond to physical security incidents. The organization monitors real-time physical intrusion alarms and surveillance equipment.	CIP-006 R4 Logging Physical Access	Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent: • Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method. • Video Recording: Electronic capture of video images of sufficient quality to determine identity. • Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in [CIP-006] Requirement R2.3.
PE-7 Visitor Control	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. The organization escorts visitors and monitors visitor activity, when required.	CIP-006 R1.4	[The Responsible Entity shall create and maintain a physical security plan…that shall address…] Procedures for the appropriate use of physical access controls as described in Requirement [CIP-006] R3 including visitor pass management….
PE-8 Access Records	The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [*Assignment: organization-defined frequency*].	CIP-006 R5 Access Log Retention	The Responsible Entity shall retain physical access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008.
PE-9 Power Equipment and Power Cabling	The organization protects power equipment and power cabling for the information system from damage and destruction.		
PE-10 Emergency Shutoff	The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.		
PE-11 Emergency Power	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.		
PE-12 Emergency Lighting	The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
PE-13 Fire Protection	The organization employs and maintains fire suppression and detection devices/ systems that can be activated in the event of a fire. The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire. The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders. The organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.		
PE-14 Temperature and Humidity Controls	The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.		
PE-15 Water Damage Protection	The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.		
PE-16 Delivery and Removal	The organization authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items.		
PE-17 Alternate Work Site	The organization employs appropriate management, operational, and technical information system security controls at alternate work sites.		
PE-18 Location of Information System Components	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.		
PE-19 Information Leakage	Control Not Selected in Moderate Baseline		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Planning			
PL-1 Security Planning Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-003 R1.1	[The Responsible Entity shall…ensure…] The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
		CIP-003 R1.3	[The Responsible Entity shall…ensure…] Annual review and approval of the cyber security policy by the senior manager assigned pursuant to [CIP-003] R2.
PL-2 System Security Plan	The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	CIP-003 R3 Exceptions	Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).
		CIP-003 R3.1	Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).
		CIP-003 R3.2	Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures, or a statement accepting risk.
PL-3 System Security Plan Update	The organization reviews the security plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system /organizational changes or problems identified during plan implementation or security control assessments.	CIP-003 R3.3	Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.
PL-4 Rules of Behavior	The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.		
PL-5 Privacy Impact Assessment	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.		
PL-6 Security-Related Activity Planning	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.	CIP-007 R1.1	The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Personnel Security			
PS-1 Personnel Security Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-004 R3 Personnel Risk Assessment	The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access….
PS-2 Position Categorization	The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [*Assignment: organization-defined frequency*].		
PS-3 Personnel Screening	The organization screens individuals requiring access to organizational information and information systems before authorizing access.	CIP-004 R3 Personnel Risk Assessment	A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include: • The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position. • The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause. • The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.
PS-4 Personnel Termination	The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.	CIP-004 R4.2	R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause
		CIP-007 R5.2.3	Where accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
PS-5 Personnel Transfer	The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.	CIP-004 R4.1	The Responsible Entity shall review the list(s) of its personnel who have access to Critical Cyber Assets and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel.
		CIP-004 R4.2	The Responsible Entity shall revoke access to Critical Cyber Assets …within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.
		CIP-007 R5.2.3	Where accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
PS-6 Access Agreements	The organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [*Assignment: organization-defined frequency*].		
PS-7 Third-Party Personnel Security	The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.	CIP-004 R4.1	The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.
PS-8 Personnel Sanctions	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
Risk Assessment			
RA-1 Risk Assessment Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	CIP-002 R1 Critical Asset Identification Method	The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.
		CIP-002 R1.1.	The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.
		CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-005 R4 Cyber Vulnerability Assessment	The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually.
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
RA-2 Security Categorization	The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.	CIP-003 R4 Information Protection	The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
		CIP-003 R4.1.	The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.
		CIP-003 R4.2	The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
RA-3 Risk Assessment	The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/ operated by external parties).	CIP-002 R1.2	The risk-based assessment shall consider the following assets: • Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard. • Transmission substations that support the reliable operation of the Bulk Electric System. • Generation resources that support the reliable operation of the Bulk Electric System. • Systems and facilities critical to system restoration, including black start generators and substations in the electrical path of transmission lines used for initial system restoration. • Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more. • Special Protection Systems that support the reliable operation of the Bulk Electric System. • Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.
		CIP-005 R4.1	• The vulnerability assessment shall include, at a minimum, a document identifying the vulnerability assessment process….
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
RA-4 Risk Assessment Update	The organization updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
RA-5 Vulnerability Scanning	The organization scans for vulnerabilities in the information system [*Assignment: organization-defined frequency*] or when significant new vulnerabilities potentially affecting the system are identified and reported.	CIP-005 R4.2 R4.3 R4.4	The vulnerability assessment shall include, at a minimum, the following: • A review to verify that only ports and services required for operations at these access points are enabled; • The discovery of all access points to the Electronic Security Perimeter; • A review of controls for default accounts, passwords, and network management community strings
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
		CIP-007 R3.1	The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
		CIP-007R8 Cyber Vulnerability Assessment	The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually.

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
System and Services Acquisition			
SA-1 System and Services Acquisition Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-003 R1.1	[The Responsible Entity shall…ensure…] The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
		CIP-003 R1.3	[The Responsible Entity shall…ensure…] Annual review and approval of the cyber security policy by the senior manager assigned pursuant to [CIP-003] R2.
SA-2 Allocation of Resources	The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.		
SA-3 Life Cycle Support	The organization manages the information system using a system development life cycle methodology that includes information security considerations.		
SA-4 Acquisitions	The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. The organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.		
SA-5 Information System Documentation	The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system. The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.		
SA-6 Software Usage Restrictions	The organization complies with software usage restrictions.		
SA-7 User Installed Software	The organization enforces explicit rules governing the installation of software by users.		
SA-8 Security Engineering Principles	The organization designs and implements the information system using security engineering principles.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
SA-9 External Information System Services	The organization: (i) requires providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.		
SA-10 Developer Configuration Management	Control Not Selected in the Moderate Baseline		
SA-11 Developer Security Testing	The organization requires information system developers create a security test and evaluation plan, implement the plan, and document the results.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
System and Communications Protection			
SC-1 System and Communications Protection Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-003 R1.1	[The Responsible Entity shall…ensure…] The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
		CIP-003 R1.3	[The Responsible Entity shall…ensure…] Annual review and approval of the cyber security policy by the senior manager assigned pursuant to [CIP-003] R2.
		CIP-005 R2 Electronic Access Controls	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s). [See also CA-3 and SC-7.]
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
SC-2 Application Partitioning	The information system separates user functionality (including user interface services) from information system management functionality.		
SC-3 Security Function Isolation	Control Not Selected in the Moderate Baseline		
SC-4 Information Remnants	The information system prevents unauthorized and unintended information transfer via shared system resources.		
SC-5 Denial of Service Protection	The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].		
SC-6 Resource Priority	Control Not Selected in the Moderate Baseline		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
SC-7 Boundary Protection	The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system. The organization physically allocates publicly accessible information system components to separate sub networks with separate, physical network interfaces. The organization prevents public access into the organization's internal networks except as appropriately mediated. The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic. The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted. The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).	CIP-005R1 Electronic Security Perimeter	The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)
		CIP-005 R1.2	For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.
		CIP-005 R1.3	Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
		CIP-005 R1.4	Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.
		CIP-005 R1.6	The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-Critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.
		CIP-005 R2 Electronic Access Controls	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s). [See also CA-3 and SC-1.]
		CIP-005 R5 Documentation Review and Maintenance R5.1	The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.
SC-8 Transmission Integrity	The information system protects the integrity of transmitted information.		
SC-9 Transmission Confidentiality	The information system protects the confidentiality of transmitted information.		
SC-10 Network Disconnect	The information system terminates a network connection at the end of a session or after [*Assignment: organization-defined time period*] of inactivity.		
SC-11 Trusted Path	The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication*].		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
SC-12 Cryptographic Key Establishment and Management	When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.		
SC-13 Use of Cryptography	For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.		
SC-14 Public Access Protections	The information system protects the integrity and availability of publicly available information and applications.		
SC-15 Collaborative Computing	The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.		
SC-16 Transmission of Security Parameters	Control Not Selected in the Moderate Baseline		
SC-17 Public Key Infrastructure Certificates	The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.		
SC-18 Mobile Code	The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of mobile code within the information system.		
SC-19 Voice Over Internet Protocol	The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of VoIP within the information system.		
SC-20 Secure Name / Address Resolution Service (Authoritative Source)	The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.		
SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver)	Control Not Selected in Moderate Baseline		
SC-22 Architecture and Provisioning for Name/Address Resolution Service	The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.		
SC-23 Session Authenticity	The information system provides mechanisms to protect the authenticity of communications sessions.		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
System and Information Integrity			
SI-1 System and Information Integrity Policy & Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	CIP-003 R1 Cyber Security Policy	The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets.
		CIP-003 R1.1	[The Responsible Entity shall…ensure…] The cyber security policy addresses the requirements in Standards CIP-002 through CIP-009, including provision for emergency situations.
		CIP-003 R1.3	[The Responsible Entity shall…ensure…] Annual review and approval of the cyber security policy by the senior manager assigned pursuant to [CIP-003] R2.
SI-2 Flaw Remediation	The organization identifies, reports, and corrects information system flaws. The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.	CIP-007 R3.2	The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.
SI-3 Malicious Code Protection	The information system implements malicious code protection. The organization centrally manages malicious code protection mechanisms. The information system automatically updates malicious code protection mechanisms.	CIP-007 R4 Malicious Software Prevention	The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
		CIP-007 R4.2	The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.
SI-4 Information System Monitoring Tools and Techniques	The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system. The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.	CIP-007 R4.1	The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.
		CIP-007 R6 Security Status Monitoring	The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
SI-5 Security Alerts and Advisories	The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.		
SI-6 Security Functionality Verification	Control Not Selected in the Moderate Baseline		
SI-7 Software and Information Integrity	Control Not Selected in the Moderate Baseline		

Table C-1. Corresponding Requirements

SP 800-53 ID	SP 800-53 Control	NERC CIP ID	NERC CIP Requirement
SI-8 Spam Protection	The information system implements spam protection.		
SI-9 Information Input Restrictions	The organization restricts the capability to input information to the information system to authorized personnel.		
SI-10 Information Accuracy, Completeness, Validity, and Authenticity	The information system checks information for accuracy, completeness, validity, and authenticity.		
SI-11 Error Handling	The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.		
SI-12 Information Output Handling and Retention	The organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.		

C.4 Operational Records and Corporate Governance Requirements

Table C-2 lists NERC CIP requirements for maintaining records that are part of operational control activities and corporate governance. These NERC CIP requirements do not correspond to any SP 800-53 controls.

Table C-2. NERC CIP Operational Records and Corporate Governance Requirements

Operational Records and Corporate Governance	
CIP-002 R2 Critical Asset Identification	The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.
CIP-003 R2 Leadership	The Responsible Entity shall assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.
CIP-003 R2.1	The senior manager shall be identified by name, title, business phone, business address, and date of designation.
CIP-003 R2.2	Changes to the senior manager must be documented within thirty calendar days of the effective date.
CIP-003 R5.1	The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.
CIP-004 R3.3	The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.
CIP-004 R4 Access	The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets
CIP-004 R1 Electronic Security Perimeter	The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
CIP-005 R2 Electronic Access Controls	The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
CIP-005 R3 Monitoring Electronic Access	The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

C.5 Redundant Requirements

Table C-3 identifies NERC CIP requirements that restate or summarize other NERC CIP requirements. They are considered redundant and are not mapped to any SP 800-53 controls.

Table C-3. Redundant NERC CIP Requirements

Redundant NERC CIP Requirements	
CIP-005 R1.5	Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007 Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.
CIP-006 R1.8	Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008, and Standard CIP-009.
CIP-007 R5.1.1	The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

Appendix D Glossary and Acronyms

D.1 Glossary

This appendix provides definitions for security terminology used in this document. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in SP 800-53.

Accreditation [FIPS 200, NIST SP 800-37]	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Authentication [FIPS 200]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).
Certification [FIPS 200, NIST SP 800-37]	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control [CNSS Inst. 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Countermeasures [CNSS Inst. 4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Controlled Area	Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

External Information System (or Component)	An information system or component of an information system that is outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service	An information system service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system).
External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
Incident [FIPS 200]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Industrial Control System	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial Control Systems include Supervisory Control and Data Acquisition (SCADA) systems used to control geographically dispersed assets, as well as Distributed Control Systems (DCS) and smaller control systems using Programmable Logic Controllers (PLC) to control localized processes.
Information Owner [CNSS Inst. 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy [CNSS Inst. 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information System [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner (or Program Manager) [CNSS Inst. 4009, Adapted]	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Label	See Security Label.
Low-Impact System [FIPS 200]	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.
Malicious Code [CNSS Inst. 4009] [NIST SP 800-61]	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Malware	See Malicious Code.
Management Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Media [FIPS 200]	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Media Sanitization [NIST SP 800-88]	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
Moderate-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Non-repudiation [CNSS Inst. 4009]	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Operational Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
Organization [FIPS 200]	A federal agency or, as appropriate, any of its operational elements.
Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Privacy Impact Assessment [OMB Memorandum 03-22]	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privileged Function	A function executed on an information system involving the control, monitoring, or administration of the system.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Remote Access	Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

Remote Maintenance	Maintenance activities conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet).
Risk [FIPS 200]	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment [NIST SP 800-30, Adapted]	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in place security controls.
Risk Management [FIPS 200]	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Safeguards [CNSS Inst. 4009, Adapted]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Security Category [FIPS 199]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Baseline [FIPS 200]	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.
Security Functions	The hardware, software, and firmware of the information system responsible for supporting and enforcing the system security policy and supporting the isolation of code and data on which the protection is based.
Security Incident	See Incident.
Security Label	Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.

Security Plan	See System Security Plan.
Security Requirements [FIPS 200]	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
System	See Information System.
System Security Plan [NIST SP 800-18, Rev 1]	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Technical Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Threat [CNSS Inst. 4009, Adapted]	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Vulnerability [CNSS Inst. 4009, Adapted]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment [CNSS Inst. 4009]	Formal description and evaluation of the vulnerabilities in an information system.

D.2 Acronyms

AGA	American Gas Association
ANSI	American National Standards Institute
API	American Petroleum Institute
CIP	Critical Infrastructure Protection
CNSS	Committee on National Security Systems
CVE	Common Vulnerabilities and Exposures
DCS	Distributed Control Systems
DHS	Department of Homeland Security
DNS	Domain Name System
DoJ	Department of Justice
DSS	Digital Signature Standard
ES ISAC	Electricity Sector Information Sharing and Analysis Center
ERO	Electric Reliability Organization
FBI	Federal Bureau of Investigation
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GCM	Galois/Counter Mode
GSA	General Services Administration
GTI	Gas Technology Institute
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HMAC	Hash Message Authentication Code
HSPD	Homeland Security Presidential Directive
ICS	Industrial Control System
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers

ISA	Instrumentation, Systems, and Automation Society
ISO	International Organization for Standardization
IT	Information Technology
MISPC	Minimum Interoperability Specification for PKI Components
MOVS	Modes of Operation Validation System
NERC	North American Electric Reliability Council
NIST	National Institute of Standards and Technology
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OMB	Office of Management and Budget
PDD	Presidential Decision Directive
PIV	Personal Identity Verification
PLC	Programmable Logic Controllers
PSRC	Power Systems Relay Committee
RFID	Radio Frequency Identification
SCADA	Supervisory Control and Data Acquisition
SEC	Security Exchange Commission
SHS	Secure Hash Standard
SP	Special Publication
TDEA	Triple Data Encryption Algorithm
TLS	Transport Layer Security
U.S.C.	United States Code
VoIP	Voice over Internet Protocol